IMS

MATHS

BOOK-09

RINGS

Defn

An algebraic structure $(R,+,\cdot)$ where R is a non-empty set and "$+$", "$\times$" are two binary operations on R, is called a ring if it satisfies the following properties:

I. $(R,+)$ is an abelian group.

(i) Closure prop:
$\forall a,b \in R \Rightarrow a+b \in R$

(ii) Associative prop:
$\forall a,b,c \in R$
$\Rightarrow (a+b)+c = a+(b+c)$

(iii) Existence of identity:
$\exists\ 0 \in R$ s.t $a+0 = 0+a = a\ \forall a \in R$
Here '0' is the identity elt in R.

(iv) Existence of inverse:
for each $a \in R$, $\exists\ -a \in R$ s.t
$a+(-a) = (-a)+a = 0$
Here $-a$ is the inverse of a in R

(v) Commutative prop:
$\forall a,b \in R \Rightarrow a+b = b+a$

II. $(R,\times)$ is a semigroup.

(i) closure prop:
$\forall a,b \in R \Rightarrow a \cdot b \in R$.

(ii) Asso. prop:
$\forall a,b,c \in R \Rightarrow (ab)c = a(bc)$

III. Distributive laws
$\forall a,b,c \in R$.

(i) $a\cdot(b+c) = a\cdot b + a\cdot c$ (LDL)

(ii) $(b+c)\cdot a = b\cdot a + c\cdot a$ (RDL)

*** Ring with unity:**

A ring R which contains the multiplicative identity (called unity) is called a ring with unity.
i.e, if $1 \in R$ s.t $a\cdot 1 = 1\cdot a = a\ \forall a \in R$
then the ring R is called a ring with unity.

*** Ring without unity:**

A ring R which does not contain multiplicative identity is called a ring without unity.

*** Commutative Ring:**

If in a ring R, the commutative property w.r.t "$\times$" is satisfied then the ring R is called commutative ring.
i.e, if $\forall a,b \in R \Rightarrow a\cdot b = b\cdot a$
then the ring R is called a commutative ring.

Defn → A ring is called finite or infinite according as it contains finite or infinite number of elements.

* Division ring (or) Skew field

If in a ring 'R', the non-zero elts form a group w.r.t x^n, a ring R is called a Division ring

(or)

A ring R is a division ring if
(i) R has atleast two elts
(ii) R has unity
(iii) Each non-zero elt of R has multiplicative inverse.

* Zero Divisor of a ring:

Let $(R,+,\cdot)$ be a ring. If there exist $a,b \in R$, where $a \neq 0$, $b \neq 0$ and $ab=0$ then R is called ring with zero divisors

(or) a, b are called zero divisors.

Here 'a' is called the left zero divisor and 'b' is called the right zero divisors.

(or)

A non-zero elt of a ring R is called a zero divisor (or) a divisor of zero if $\exists$ an elt $b \neq 0 \,(\in R)$ s.t either $ab=0$ or $ba=0$

* Ring without zero divisors:-

A ring which is not with zero divisor is called ring without zero divisor.

i.e, if $a \neq 0$, $b \neq 0$ then $ab \neq 0$

(or)

A ring R is said to have no zero divisors if $a,b \in R$ and $ab=0 \Rightarrow a=0$ (or) $b=0$

Ex (1) The ring of integers Z has no zero divisors.

for $a,b \in Z$ and $ab=0$
$\Rightarrow a=0$ or $b=0$

(2) The ring $(R,+,\cdot)$ where $R=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5}\}$ has zero divisors.

i.e, $\underset{\neq 0}{\bar{2}}, \underset{\neq 0}{\bar{3}} \in R \Rightarrow \bar{2}\cdot\bar{3}=0$.

(3) The ring $(R,+,\cdot)$ where R = set of 2x2 matrices whose elts are real numbers has zero divisors.

Since $A=\begin{bmatrix}1&0\\0&0\end{bmatrix} \neq 0$, $B=\begin{bmatrix}0&0\\0&1\end{bmatrix} \neq 0 \in R$

$\Rightarrow AB=\begin{bmatrix}0&0\\0&0\end{bmatrix}$
$=0$

* Integral Domain

A Commutative Ring with unity and without zero divisors is called an I.D.

i.e, A ring R is an Integral domain if (i) R is commutative
(ii) R has unity
(iii) R is without zero divisors.

* Field:

A commutative division ring is called field.

i.e, A Ring R is said to be a field if it has atleast two elts and (i) is commutative
(ii) has unity
(iii) Every non-zero elt of R is invertible w.r.t x^n.

* Some elementary properties of Rings:

Theorem If R is a ring and $0, a, b \in R$ then (i) $0a = a0 = 0$
(ii) $a(-b) = (-a)(b) = -(ab)$
(iii) $(-a)(-b) = ab$ and
(iv) $a(b-c) = ab - ac$

Proof (i) $0a = (0+0)a$

$0 + 0a = 0a + 0a$ (By RDL)

$\Rightarrow 0 = 0a$ (By RCL)

Similarly we can prove that $a0 = 0$

$\therefore 0a = a0 = 0$

(ii) To prove that $a(-b) = -(ab)$

Now we have $a0 = a(-b+b)$

$\Rightarrow a(-b+b) = a0$

$\Rightarrow a(-b) + ab = 0$ (by (i) & LDL)

$\Rightarrow a(-b) = -(ab)$

Similarly we can prove that $(-a)b = -(ab)$.

$\therefore a(-b) = (-a)b = -(ab)$

(iii) $(-a)(-b) = -[(-a)b]$ [by (ii)]

$= -[-(ab)]$ (by (ii))

$= ab$

(iv) $a(b-c) = a[b+(-c)]$

$= ab + a(-c)$ (by LDL)

$= ab - ac$ (by (ii))

Theorem If R is a ring with unit elt and $a \in R$ then (i) $(-1)a = -a$
(ii) $(-1)(-1) = 1$

Proof (i) Now we have

$0a = (-1+1)a$

$\Rightarrow (-1+1)a = 0a$

$\Rightarrow (-1)a + (1)a = 0$

$\Rightarrow (-1)a + a = 0$

$\Rightarrow (-1)a = -a$

(ii) for $a \in R$, we have $(-1)a = -a$

Taking $a = -1$

$\therefore (-1)(-1) = -(-1)$

$\Rightarrow (-1)(-1) = 1$

Examples:-

(1) Let $R = \{0\}$ and $+, \cdot$ be the binary operations defined by $0+0=0$ and $0 \cdot 0 = 0$ then $(R, +, \cdot)$ is clearly a ring, called the null ring or zero ring

(2) I = the set of integers

I. (i) $\forall a,b \in I \Rightarrow a+b \in I$

$\therefore$ Closure property is satisfied.

(ii) $\forall a,b,c \in I$

$\Rightarrow (a+b)+c = a+(b+c)$

$\therefore$ Asso. prop. is satisfied

(iii) $\exists\, 0 \in I$ s.t $a+0=0+a=a \ \forall a \in R$

Identity elt $= 0 \in I$

$\therefore$ Identity prop. is satisfied

(iv) $\forall a \in I \ \exists -a \in I$ s.t $a+(-a) = (-a)+a = 0$

$\therefore$ '$-a$' is the inverse of 'a' in I

Inverse prop. is satisfied.

(v) $\forall a,b \in I \Rightarrow a+b = b+a$

$\therefore$ Commutative property is satisfied.

$\therefore (I,+)$ is an abelian group

II. (i) $\forall a,b \in I \Rightarrow a.b \in I$

Closure prop. is satisfied

(ii) $\forall a,b,c \in I$

$\Rightarrow (a.b).c = a.(b.c)$

$\therefore (I,\cdot)$ is a semigroup.

III. $\forall a,b,c \in I$

(i) $a\cdot(b+c) = ab+ac$ (LDL)

(ii) $(b+c).a = ba+ca$ (RDL)

$\therefore$ Distributive laws are satisfied.

$\therefore (I,+,\cdot)$ is a ring.

IV. $\exists\, 1 \in I$ s.t $a.1 = 1.a = a \ \forall a \in I$

$\therefore$ Identity elt $= 1 \in I$

$\therefore (I,+,\cdot)$ is a ring with unity

V. $\forall a,b \in I \Rightarrow a.b = b.a$

$\therefore$ comm. prop. is satisfied.

$(I,+,\cdot)$ is a comm. ring with unity.

VI. $\forall a,b \in I$

$a.b = 0 \Rightarrow a=0$ or $b=0$

$\therefore I$ does not contain zero divisors.

$\therefore (I,+,\cdot)$ is an integral domain.

VII. $\forall a \neq 0 \in I \ \exists \frac{1}{a} \notin I$ s.t $a.\frac{1}{a} = \frac{1}{a}.a = 1$

Inverse prop. is not satisfied. w.r.t $\times^n$.

$\therefore (I,+,\cdot)$ is not a field.

(3) The set N of natural numbers is not a ring w.r.t. $+^n$ & $\times^n$. because $(N,+)$ is not group.

(4) I_E = The set of even integers including zero is a commutative ring

(5) The sets Q, R, C are fields.

(6) The set of irrational numbers under $+^n$ & $\times^n$ is not a ring.

(6) The set M of all $n\times n$ matrices with their elts as real numbers (rational numbers, complex numbers, integers) is a non-commutative ring with unity w.r.t. $+^n$ & $\times^n$.

Sol^n

I. (i) $\forall A, B \in M$
$\Rightarrow A+B \in M$
Closure prop. is satisfied.

(ii) $\forall A, B, C \in M$
$(A+B)+C = A+(B+C)$
$\therefore$ Asso. prop. is satisfied.

(iii) $\exists B = O_{n\times n} \in M$ s.t
$A+B = B+A = A \quad \forall A \in M$
Identity elt $= O_{n\times n} \in M$
$\therefore$ Identity prop is satisfied.

(iv) $\forall A \in M \ \exists -A \in M$
s.t $A+(-A) = (-A)+A = O$
$\therefore$ Inverse of A is $-A$.
$\therefore$ Inverse prop. is satisfied

(v) $\forall A, B \in M \Rightarrow A+B = B+A$
$\therefore$ Commutative prop. is satisfied.

II. (i) $\forall A, B \in M \Rightarrow AB \in M$
$\therefore$ Closure prop. is satisfied.

(ii) $\forall A, B, C \in M$
$\Rightarrow (A\cdot B)C = A(B\cdot C)$.
$\therefore$ Asso. prop. is satisfied.

III. $\forall A, B, C \in M$
(i) $A\cdot(B+C) = AB+AC$
(ii) $(B+C)\cdot A = BA+CA$.
$\therefore$ Distributive laws satisfied.
$\therefore (M, +, \cdot)$ is a ring.

IV. $\exists B = I$ (unit Matrix) $\in M$
s.t $A\cdot B = B\cdot A = A, \forall A \in M$
$\therefore$ identity elt $= I$ (Identity matrix)
$\therefore (M, +, \cdot)$ is a ring with unity.

V. $\forall A, B \in M$
$\Rightarrow A\cdot B \neq B\cdot A$.
$\therefore$ Commutative prop. is not satisfied w.r.t $\times^n$.

$\therefore (M, +, \cdot)$ is non-commutative ring with unity.

(7) $F = \{ b\sqrt{2} \mid b$ is a rational number$\}$

Sol^n Let $a\sqrt{2}, b\sqrt{2} \in F$ where $a, b \in Q$
$\Rightarrow a\sqrt{2}+b\sqrt{2} = (a+b)\sqrt{2} \in F$
$(\because a+b \in Q)$
Closure prop. is satisfied w.r.t $+^n$.
$\therefore +^n$ is a binary operation on F.

(ii) Let $a\sqrt{2}, b\sqrt{2} \in F$; $a, b \in Q$
$\Rightarrow a\sqrt{2}\cdot b\sqrt{2} = ab(2) \notin F$.
$\therefore \times^n$ is not b.o. on F.

(8) $Q[\sqrt{2}] = \{a+b\sqrt{2} / a, b \in Q\} \subseteq R$.
$+^n$ & $\times^n$ b–o's on F.

Sol I.
(i) Closure prop:
Let $a+b\sqrt{2}, c+d\sqrt{2} \in F$
$a, b, c, d \in Q$
$(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in F$
$(\because a+c, b+d \in Q)$
$\therefore$ Closure prop. is satisfied.

(ii) Asso. prop:
Let $x, y, z \in F \subseteq R$.
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}, z = e+f\sqrt{2}$
where $a, b, c, d, e, f \in Q$
$\therefore (x+y)+z = x+(y+z)$ (by Asso. prop. of R)
$\therefore$ Asso. prop. is satisfied.

(iii) Existence of left identity
$\forall\, x = a+b\sqrt{2} \in F$, where $a, b \in Q$, $\exists\, y = 0+0\sqrt{2} \in F$, $0 \in Q$
s.t $y + x = (0+0\sqrt{2}) + (a+b\sqrt{2})$
$= (0+a) + (0+b)\sqrt{2}$
$= a+b\sqrt{2}$ $0+a \in Q$, $0+b \in Q$
$= x$.
$\therefore$ The identity elt $= 0+0\sqrt{2}$
$= 0$ is in F.

(iv) Existence of left inverse:
$\forall\, a+b\sqrt{2} \in F$, $a, b \in Q$, $\exists\, -a-b\sqrt{2} \in F$, $-a, -b \in Q$.
s.t $(-a-b\sqrt{2}) + (a+b\sqrt{2}) = (-a+a) + (-b+b)\sqrt{2}$
$= 0 + 0\sqrt{2} = 0$
$(\because -a+a = 0, -b+b = 0)$
$\therefore$ Inverse of $a+b\sqrt{2} = -a-b\sqrt{2} \in F$.

(v) Commutative property,
~~$\forall\, x, y \in F \subseteq R$.~~
$\Rightarrow x+y = y+x$ (by comm. prop. of R)
$\therefore$ Comm. prop. is satisfied.
$(F, +)$ is an abelian group.

II. (i) Closure prop.
Let $x = a+b\sqrt{2}, y = c+d\sqrt{2} \in F$; $a, b, c, d \in Q$
then $x \cdot y = (a+b\sqrt{2})(c+d\sqrt{2})$
$= (ac+2bd) + (ad+bc)\sqrt{2} \in F$
$(\because ac+2bd, ad+bc \in Q)$
$\therefore$ Closure prop. is satisfied.

(ii) Let $x, y, z \in F \subseteq R$
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}, z = e+f\sqrt{2}$; $a, b, c, d, e, f \in Q$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (by asso. prop. of R)
$\therefore$ Asso. prop. is satisfied.
$\therefore (F, \cdot)$ is a semi group.

III. Let $x, y, z \in F \subseteq R$
$x \cdot (y+z) = x \cdot y + x \cdot z$ (by LDL of R)
$(y+z) \cdot x = y \cdot x + z \cdot x$ (by RDL of R)
$\therefore$ Distributive laws are satisfied.
$\therefore (F, +, \cdot)$ is a ring.

IV. Identity prop.:
$\exists\, 1+0\sqrt{2} = 1 \in F$; $0, 1 \in Q$
s.t $(1+0\sqrt{2})(a+b\sqrt{2}) = a+b\sqrt{2}$
$\forall\, a+b\sqrt{2} \in F$, $a, b \in Q$
$\therefore$ Identity elt w.r.t. $\times^n$ is 1
$= 1+0\sqrt{2} \in F$
$\therefore$ Identity prop. is satisfied.
$(F, +, \cdot)$ is a ring with unity.

V. Commutative prop.
Let $x, y \in F \subseteq R$
Choosing $x = a+b\sqrt{2}, y = c+d\sqrt{2}$, $a, b, c, d \in Q$

$\therefore x\cdot y = y\cdot x$ (by comm. prop. of R)

$\therefore$ Comm. prop. is satisfied in F.

$\therefore (F,+,\cdot)$ is a commutative ring with unity

VI. Let $x, y \in F \subseteq R$

Choosing $x = a+b\sqrt{2},\ y = c+d\sqrt{2}$, $a,b,c,d \in Q$

$\therefore x\cdot y = 0 \Rightarrow x = 0$ or $y = 0$

$\therefore F$ doesnot contain zero divisors.

$\therefore (F,+,\cdot)$ is an integral domain.

VII. Let $a+b\sqrt{2} \neq 0 \in F$, $a \neq 0$, or $b \neq 0 \in Q$

s.t $(c+d\sqrt{2})(a+b\sqrt{2}) = 1$

$$\Rightarrow c+d\sqrt{2} = \frac{1}{a+b\sqrt{2}}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} - \frac{b(\sqrt{2})}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} + \left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \in F$$

$\left(\because \frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in Q \ \&\ a^2-2b^2 \neq 0\right)$

$\therefore \exists\ \frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in F \subseteq R$

s.t $\left(\frac{a}{a^2-2b^2} + \frac{(-b)}{a^2-2b^2}\sqrt{2}\right)(a+b\sqrt{2}) = 1$ $\forall\, a+b\sqrt{2} \in F$

$\therefore$ Inverse of $a+b\sqrt{2}$ is $\frac{a}{a^2-2b^2} + \frac{(-b)\sqrt{2}}{a^2-2b^2} \in F$.

$\therefore$ Every non-zero elt of F has inverse w.r.t $\times^n$.

$\therefore$ Inverse of prop. is satisfied.

$\therefore (F,+,\cdot)$ is a field.

H.W $\rightarrow F = Z(\sqrt{2}) = \left\{a+b\sqrt{2} \,/\, a, b \text{ are integers}\right\} \subseteq R$

$(F,+,\cdot)$ is an I.D. but not field.

H.W $\rightarrow F = J[i]$ = the set of Gaussian integers;
$= \{a+bi \,/\, a,b \in I\} \subseteq C$

$(F,+,\cdot)$ is ~~I.D~~ but not field

$\rightarrow$ show that the set of integers I with two binary operations '$*$' and '$\circ$' defined by $a*b = a+b-1$, $a\circ b = a+b-ab$ $\forall a,b \in I$ is comm. ring.

Sol^n: $\forall\ a,b \in I$

$a*b = a+b-1$ —(1)

and $a\circ b = a+b-ab$ —(2)

I. from (1)

(i) we have $a*b = a+b-1 \in I$

$\therefore *$ is closed in I.

(ii) $\forall\ a,b,c \in I$

$(a*b)*c = a*(b*c)$.

Since $(a*b)*c = (a+b-1)*c$
$= (a+b-1)+c-1$
$= a+b+c-2$

$a*(b*c) = a*(b+c-1)$
$= a+(b+c-1)-1$
$= a+b+c-2$

∴ Asso. prop. is satisfied.

(iii) Existence of left identity:

$\forall a \in I \ \exists b \in I$ s.t $b*a = a$
$\Rightarrow b+a-1 = a$
$\Rightarrow b = 1$

∴ $\forall a \in I \ \exists 1 \in I$ s.t $1*a = a$

∴ 1 is the identity in I w.r.t $*$

(iv) Existence of left inverse

$\forall a \in I \ \exists b \in I$ s.t $b*a = 1$
$\Rightarrow b+a-1 = 1$
$\Rightarrow b = 2-a \in I$

∴ $\forall a \in I \ \exists b = 2-a \in I$
s.t $(2-a)*a = 1$

∴ $b = 2-a$ is the inverse of 'a' in I w.r.t $*$.

(v) Comm. prop:

$\forall a,b \in I$, $a*b = b*a$

Since $a*b = a+b-1$
$= b+a-1$
$= b*a$.

∴ $*$ is commutative in I.

∴ $(I,*)$ is abelian group.

II. from (2) (i) Closure prop.

$\forall a,b \in I$, $a \circ b = a+b-ab \in I$

∴ '$\circ$' is closed in I

(ii) $\forall a,b,c \in I$

$a \circ (b \circ c) = (a \circ b) \circ c$.

Since $(a \circ b) \circ c = (a+b-ab) \circ c$
$= (a+b-ab) + c - (a+b-ab)c$
$= a+b+c-ab-ac-bc+abc$

and $a \circ (b \circ c) = a \circ (b+c-bc)$
$= a+(b+c-bc) - a(b+c-bc)$
$= a+b+c-ab-bc-ac+abc$.

∴ '$\circ$' is associative in I.

∴ $(I,\circ)$ is ~~a semi group~~.

III. Left distributive law

$\forall a,b,c \in I \Rightarrow a \circ (b*c) = a \circ [b+c-1]$
$= a+(b+c-1) - a(b+c-1)$
$= a+b+c-1-ab-ac+a$
$= (a+b-ab)+(a+c-ac)-1$
$= (a \circ b) + (a \circ c) - 1$
$= (a \circ b) * (a \circ c)$.

∴ Distributive law is satisfied.

∴ $(I,*,\circ)$ is a ring.

IV. Comm. prop

$\forall a,b \in I$
$\Rightarrow a \circ b = a+b-ab$
$= b+a-ba$
$= b \circ a$

∴ '$\circ$' is commutative in I.

∴ $(I,*,\circ)$ is a commutative ring.

H.W. If $(R,+,\cdot)$ is a ring with unit elt. Show that $(R,\oplus,\otimes)$ is also a ring with unit elt, where $a \oplus b = a+b+1$ & $a \otimes b = ab+a+b$ $\forall a,b \in R$.

H.W. If E denotes the set of even integers, then prove that $(E,+,*)$ is a commutative ring. Where $a*b = \frac{ab}{2}$ and '+' is usual addition.

H.W. P.T the set 'S' of all ordered pairs (a,b) of real numbers is a commutative ring under $+^n$ & $\times^n$ composition defined as

$(a,b)+(c,d) = (a+c, b+d)$ and
$(a,b)(c,d) = (ac, bd)$

Defn Cancellation laws in a Ring:

In a ring R, for $a,b,c \in R$ if $a \neq 0$, $ab = ac \Rightarrow b = c$ (LCL)

and $a \neq 0$, $ba = ca \Rightarrow b = c$ (RCL).

then we say that cancellation laws hold in R.

Theorem 2004. A ring R is without zero divisors iff the cancellation laws hold in R.

proof: Let the ring R will have no zero divisors

To prove that the cancellation laws hold in R.

Let $a, b, c \in R$ and $a \neq 0$,

we have $ab = ac$

$\Rightarrow ab + (-ac) = 0$

$\Rightarrow$ ~~$ab + a(-c) = 0$~~

$\Rightarrow a[b + (-c)] = 0$

$\Rightarrow a(b - c) = 0$

$\Rightarrow b - c = 0 \quad (\because a \neq 0)$

$\Rightarrow b = c$.

Similarly we prove that $a, b, c \in R$ and $a \neq c$, $ba = ca \Rightarrow b = c$.

Conversely suppose that the cancellation laws hold in R. we have to prove that R has no zero divisors.

If possible suppose that R has zero divisors.

then $\exists\ a, b \in R$ such that $a \neq 0, b \neq 0$ and $ab = 0$.

Now we have $a \neq 0, ab = 0$

$\Rightarrow a \neq 0, ab = a0$

$\Rightarrow b = 0$ (by LCL)

which is a contradiction.

$\therefore$ R has no zero divisors.

→ If R is a ring with unit element and $x \neq 0 \in R$ and a unique element $y \in R$ exists such that $xyx = x$. Show that $xy = yx = 1$.

Sol^n: $x \neq 0$ and $xyx = x$

$\Rightarrow x \neq 0$ and $(xy)x = 1.x$

$\Rightarrow xy = 1$ (by RCL)

Now $x \neq 0$ and $xyx = x$

$\Rightarrow x \neq 0$ and $x(yx) = x.1$

$\Rightarrow yx = 1$ (by LCL)

$\therefore xy = yx = 1$

$(xy)x - 1x = 0$

$(xy - 1)x = 0$

$xy - 1 = 0$ ($\because x \neq 0$)

$xy = 1$

Theorem → Let R be a commutative ring with unity. Then R is an ID iff $ab = ac \Rightarrow b = c$ where $a, b, c \in R$ and $a \neq 0$

(or) —

A commutative ring R with unity is an ID iff the cancellation laws hold in R.

proof: Suppose R is an ID then we have to show that the cancellation laws hold in R.

Let $a, b, c \in R$ and $a \neq 0$.

we have $ab = ac$

$\Rightarrow a(b-c) = 0$ —— (1)

Since R is ID.

i.e., R is a commutative ring with unity and has no zero divisors.

$\therefore$ from ①, either $a=0$ or $b-c=0$

but it is given that $a\neq 0$.

$\therefore b-c=0$

$\Rightarrow b=c$

Similarly we prove that, $a,b,c\in R$, $a\neq 0$,

$ba=ca \Rightarrow b=c$

$\therefore$ The cancellation laws hold in R.

Conversely suppose that the cancellation laws hold in R.

we prove that R is an I.D.

for this we are enough to prove that R has no zero divisors.

If possible let R has zero divisors. then

$\exists\, a,b\in R$ such that $a\neq 0$, $b\neq 0$ and $ab=0$

Now we have $a\neq 0$, $ab=0$

$\Rightarrow a\neq 0$, $ab=a0$

$\Rightarrow b=0$ (By LCL)

which is contradiction

$\therefore R$ has no zero divisors.

$\therefore R$ is an I.D.

Note: The cancellation laws may not hold in an arbitrary ring.

Let $A=\begin{bmatrix}1&1\\1&1\end{bmatrix}$, $B=\begin{bmatrix}2&0\\0&2\end{bmatrix}$ and $C=\begin{bmatrix}1&0\\1&0\end{bmatrix}$ be three elements in the ring M_2 of all 2×2 matrices over the integers. Then $AC=\begin{bmatrix}2&0\\2&0\end{bmatrix}=BC$ but $A\neq B$.

Theorem A divison ring has no zero divisors.

proof: Let $(R,+,\cdot)$ be a divison ring.

i.e, in a ring R, the non-zero elements form a group w.r.t $\times^n$.

Let $a,b \in R$ and $a \neq 0$.

Since R is a divison ring.

For $a \neq 0 \in R \Rightarrow a^{-1}$ exists in R.

$\therefore a a^{-1} = a^{-1} a = 1$.

Now we have $ab = 0$

$\Rightarrow a^{-1}(ab) = a^{-1} \cdot 0$

$\Rightarrow (a^{-1}a)b = 0$

$\Rightarrow 1b = 0$

$\Rightarrow b = 0$

$\therefore a,b \in R, a \neq 0$ and $ab = 0 \Rightarrow b = 0$.

Similarly we can prove that $a,b \in R, b \neq 0$ and $ab = 0 \Rightarrow a = 0$

$\therefore a,b \in R$ and $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

$\therefore R$ has no zero divisors.

Theorem A field has no zero divisors

proof: Same as the proof of the above theorem

Defn:

The pigeon-Hole principle: If 'n' objects are distributed over x places in such a way that no place receives more than one object then each place receives exactly one object.

Theorem Every field ~~is an~~ I.D.

proof: Let F be a field then by defn F is a commutative ring with unity and every non-zero elt is invertible w.r.t $\times^n$.

In order to prove that a field is an I.D.

we have to prove that a field F has no zero divisors.

Let $a,b \in F$ and $a \neq 0$.

since F is a field.

for $a \neq 0 \in F \Rightarrow a^{-1}$ exists in F.

$\therefore a a^{-1} = a^{-1} a = 1$

Now we have

$ab = 0$

$\Rightarrow a^{-1}(ab) = a^{-1} 0$

$\Rightarrow (a^{-1}a) b = 0$

$\Rightarrow 1b = 0$

$\Rightarrow b = 0$

Similarly we can prove that $a, b \in F$.

$b \neq 0$ and $ab = 0 \Rightarrow a = 0$.

$\therefore a, b \in F$ and $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

$\therefore F$ has no zero divisors.

$\therefore$ A field is an ID.

Note: The converse of the above need not be true.

i.e., every ID need not be a field.

Ex: The ring of integers $(Z, +, \cdot)$ is an ID but not field. because $2(\neq 0) \in Z$ has no $\times^{ve}$ inverse.

Theorem (2007): A finite integral domain is a field.

proof: Let F be the finite ID.

Let $F = \{a_1, a_2, \ldots\ldots a_n\}$ and F contains 'n' distinct elements.

To prove that F is a field.

for this we are enough to prove that the non-zero elements of F have x^{ve} inverse.

Let $a \neq 0 \in F$

$\therefore aa_1, aa_2, \ldots\ldots aa_n \in F$ (by Closure prop.)

All these elements are distinct.

because: If possible

let $aa_i = aa_j$; $a_i, a_j \in F$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is an ID i.e., F does not contain zero divisors.)

$\Rightarrow a_i = a_j$

This is a contradiction to hypothesis that F contains n distinct elements.

$\therefore$ Our assumption that $aa_i = aa_j$ is wrong.

$\therefore aa_1, aa_2, \ldots\ldots aa_n$ are all distinct elements in F which has exactly 'n' elements.

By the pigeon-hole principle, one of these products must be equal to one. ($\because$ F is a ID)

Let $aa_r = 1$ for some $a_r \in F$.

$\therefore a^{-1} = a_r$.

$\therefore$ Every non-zero element of F has x^{ve} inverse.

$\therefore$ F is a field.

Theorem (2000) A finite commutative ring without zero divisors is a field.

proof: Let F be a finite commutative ring without zero divisors.

Let $F = \{a_1, a_2, \ldots\ldots a_n\}$ and F contains 'n' distinct elements.

To prove that F is a field.

For this we are enough to prove that an element $1 \in F$ such that $1 \cdot a = a \cdot 1 = a$ $\forall a \in F$ and also for every element $a \neq 0 \in F$, there exists an element $b \in F$ such that $ab = ba = 1$.

Let $a \neq 0 \in F$.

$\therefore aa_1, aa_2, \ldots, aa_n \in F$ (by closure prop of F)

All these elts are distinct.

because, If possible let $aa_i = aa_j$; $a_i, a_j \in R$

$\Rightarrow a(a_i - a_j) = 0$

$\Rightarrow a_i - a_j = 0$ ($\because a \neq 0$ & F is ID)

$\Rightarrow a_i = a_j$ which is contradiction to hyp. that F contains n distinct elts.

$\therefore aa_1, aa_2, \ldots, aa_n$ are all distinct elts in F which has exactly 'n' elts.

By the pigeon-hole principle every element F can be written as aa_i for some $a_i \in F$.

Since $a \neq 0 \in F$, we have $a = aa_i$ for some $a_i \in F$.

Since F is commutative:

$\therefore a = aa_i = a_i a$.

We now prove that a_i is unit element.

Let $y \in F$ then $y = aa_j$ for some $a_j \in F$.

$\Rightarrow a_i y = a_i(aa_j)$

$= (a_i a) a_j$

$= aa_j$

$= y$

$\Rightarrow a_i y = 1 \cdot y \Rightarrow a_i = 1$ (by RCL)

$\therefore a \in F$ $\exists$ $1 \in F$ such that $a \cdot 1 = 1 \cdot a = a$

$\therefore$ 1 is the unit element in F.

Since $1 \in F$

$1 = a a_k$ for some $a_k \in F$.

$\therefore$ For $a \neq 0 \in F$, $\exists a_k \in F$ such that $a a_k = 1 = a_k a$ ($\because$ F is comm.)

$\therefore a \neq 0 \in D$ has x^{ve} inverse in F.

$\therefore$ F is a field.

$F = (\{0,1,2,3,4,5\}, +_6, \times_6)$

Sol^n Form the composition tables for F w.r.t $+_6$ & $\times_6$.

table(i)

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

table (ii)

$\times_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(I) (i) From table (i)

Closure prop: All the elements of the composition table are elements of set F.

$\therefore$ Closure prop. is satisfied.

(ii) Asso. prop:

$2, 4, 5 \in F \Rightarrow (2 +_6 4) +_6 5 = 2 +_6 (4 +_6 5)$.

Since $(2 +_6 4) +_6 5 = 0 +_6 5 = 5$

and $2 +_6 (4 +_6 5) = 2 +_6 3 = 5$.

$\therefore \forall a, b, c \in F \Rightarrow (a +_6 b) +_6 c = a +_6 (b +_6 c)$

$\therefore$ Asso. prop is satisfied.

(iii) The first row of table (i) coincides with the top row.

∴ The element in the extreme left coloumn of the first row i.e, '0' is the identity element.

∴ Identity prop. is satisfied.

(iv) Every row & coloumn contains the identity element '0'.

∴ Inverse prop is satisfied.

Here $0 +_6 0 = 0$, inverse of 0 is 0

$1 +_6 5 = 5 +_6 1 = 0$, inverse of 5 is 1
" " 1 is 5

$2 +_6 4 = 4 +_6 2 = 0$, inverse of 4 is 2
" " 2 is 4.

$3 +_6 3 = 3 +_6 3 = 0$ inverse of 3 is 3.

(v) Interchanging the rows and coloumns. There is no change in the table.

∴ Comm. prop is satisfied.

∴ $(F, +)$ is an abelian group.

(II) From the table (ii)

(i) Closure prop: All the entries of the composition table are the elements of the set F.

∴ Closure prop is satisfied.

(ii) $2, 3, 5 \in F$

$(2 \times_6 3) \times_6 5 = 2 \times_6 (3 \times_6 5)$

Since $(2 \times_6 3) \times_6 5 = 0 \times_6 5 = 0$

and $2 \times_6 (3 \times_6 5) = 2 \times_6 3 = 0$

∴ $\forall a, b, c \in F \Rightarrow (a \times_6 b) \times_6 c = a \times_6 (b \times_6 c)$.

∴ Asso. prop. is satisfied.

(iii) Distributive laws:

$2,3,5 \in F$.

$\Rightarrow 2\times_6(3+_6 5) = (2\times_6 3) +_6 (2\times_6 5)$.

Since $2\times_6(3+_6 5) = 2\times_6(2) = 4$

and $(2\times_6 3) +_6 (2\times_6 5) = 0 +_6 4 = 4$

Similarly $(3+_6 5)\times_6 2 = (3\times_6 2) +_6 (5\times_6 2)$

$\therefore \forall a,b,c \in F$

$\Rightarrow a\times_6(b+_6 c) = (a\times_6 b) +_6 (a\times_6 c)$.

& $(b+_6 c)\times_6 a = (b\times_6 a) +_6 (c\times_6 a)$.

$\therefore$ Distributive laws are satisfied.

$(F, +_6, \times_6)$ is a ring.

(iv) Identity property:

From the table (ii), the second row coincides with the top row.

$\therefore$ The element in extreme left coloumn of second row i.e, 1 is the Identity element.

$\therefore$ Identity prop. is satisfied.

$\therefore (F, +_6, \times_6)$ is a ring with unity.

(v) from table (ii),

- interchanging rows and columns, there is no
- change in the table.

$\therefore$ Comm. prop is satisfied w.r.t $\times^n$.

(vi) from table (ii),

$2\neq 0, 3\neq 0$, but $2\times_6 3 = 0$

$3\neq 0, 4\neq 0$ but $3\times_6 4 = 0$

$\therefore a\neq 0, b\neq 0 \in F \Rightarrow a\times_6 b = 0$.

$\therefore$ F contains zero divisors.

$\therefore (F, +_6, \times_6)$ is not an ID.

(VII) From the table (iii),
$3^{rd}, 4^{th}, 5^{th}$ rows & columns donot contain identity element 1.
$\therefore$ Inverses 2, 3, 4 donot exist.
$\therefore$ ~~Inverse prop is satisfied.~~
$\therefore$ $(F, +_6, \times_6)$ is not a field.

Theorem $\rightarrow$ Let p be a prime number. prove that the set of integers I_p,
$I_p = \{0, 1, 2, 3, \ldots\ldots p-1\}$ forms a field w.r.t $+^n$ & $\times^n$ modulo p.

proof: (I) If $a, b \in I_p$ and p is +ve integer then $a +_p b \equiv r$, ~~where r is~~ the remainder when $a+b$ is divided by p.
Clearly $0 \le r \le p-1 < p$.

(i) closure prop:
$\forall a, b \in I_p \Rightarrow a +_p b \in I_p$
Since $a +_p b = r$; $0 \le r < p$.
$\therefore$ $+_p$ is closed in I_p.

(ii) Asso. prop:
$\forall a, b, c \in I_p$
$\Rightarrow a +_p (b +_p c) = (a +_p b) +_p c$.
Since $a +_p (b +_p c) = a +_p (b + c)$

$(\because b +_p c \equiv b + c \pmod p$
i.e, $a + b \equiv r \pmod p$
i.e, $12 +_4 7 \equiv 1 \cdot 2 + 7 \pmod 4$
$3 \equiv 19 \pmod 4)$

$= $ remainder when $a+(b+c)$ is divided by p.

$=$ remainder when $(a+b)+c$ is divided by p.

$= (a+b)+_p c$ (by def of $+_p$)

$= (a +_p b) +_p c$ $\quad (\because a+b \equiv a +_p b \pmod p$.

$\therefore +_p$ is associative in I_p.

(iii) Existence of identity

Let $a \in I_p$ $\exists\, 0 \in I_p$ such that $0 +_p a = a +_p 0 = a$

$\therefore 0$ is the identity element in I_p.

(iv) Existence of inverse:

Since $0 +_p 0 = 0$.

$\therefore$ The inverse of 0 is 0 itself.

if $r (\neq 0) \in I_p$ then $p - r \in I_p$

$\therefore (p-r) +_p r =$ remainder 0 when $(p-r)+r$ is divided by p.

$= r +_p (p-r)$.

$\therefore p - r$ is the inverse of 'r'

i.e, every element in I_p has inverse

$\therefore$ Inverse prop. is satisfied w.r.t $+_p$.

(v) Comm. prop:

$\forall a, b \in I_p \Rightarrow a +_p b = b +_p a$.

Since $a +_p b =$ remainder when $a+b$ is divided by p.

$=$ remainder when $b+a$ is divided by p.

$= b +_p a$.

$\therefore (I_p, +_p)$ is an abelian group.

II Let $a, b \in I_p$ then $a \times_p b = r$ where 'r' is the remainder when ab is divided by p. and $0 \le r < p$.

(i) $\forall a, b \in I_p$

$\Rightarrow a \times_p b \in I_p$

Since $a \times_p b = r;\ 0 \le r < p$.

$\therefore \times_p$ is closed on I_p.

(ii) $\forall a, b, c \in I_p$

$\Rightarrow a \times_p (b \times_p c) = (a \times_p b) \times_c c$

Since $a \times_p (b \times_p c) = a \times_p (bc)$

$(\because b \times_p c \equiv bc \pmod p)$

= remainder when $a(bc)$ is divided by p.

= remainder when $(ab)c$ is divided by p.

$= (ab) \times_p c$.

$= (a \times_p b) \times_p c$.

$\therefore \times_p$ is associative on I_p.

$\therefore (I_p, \times_p)$ is a semi group.

(iii) Let $a, b, c \in I_p$ then

$a \times_p (b +_p c) = a \times_p (b + c)$

$(\because b +_p c \equiv b + c \pmod p)$

= remainder when $a(b+c)$ is divided by p.

= remainder when $(ab + ac)$ is divided by p.

$= (ab) +_p (ac)$

$= (a \times_p b) +_p (a \times_p c)$ $(\because ab \equiv a \times_p b)$

$\therefore a \times_p (b +_p c) = (a \times_p b) +_p (a \times_p c)$

Similarly $(b +_p c) \times_p a = (b \times_p a) +_p (c \times_p a)$

$\therefore$ Distributive laws are satisfied.

i.e, $\times_p$ is distributive w.r.t $+_p$ on P.

$\therefore (I_p, +_p, \times_p)$ is a ring.

(IV) Let $\forall a, b \in I_p$; Then $a \times_p b = b \times_p a$

Since $a \times_p b$ = remainder when ab is divided by p.

= remainder when ba is divided by p.

$= b \times_p a$

$\therefore \times_p$ is Comm. on I_p.

$\therefore (I_p, +_p, \times_p)$ is a comm. ring ~~with unity~~.

(V) $\exists\ 1 \in I_p$ such that $a \times_p 1 = 1 \times_p a = a\ \forall a \in I_p$.

$\therefore$ 1 is the identity element w.r.t $\times$?

(VI) Let $a, b \in I_p$ then $a \times_p b = 0$

$\Rightarrow ab$ is divided by p. i.e, $\frac{ab}{p}$.

$\Rightarrow \frac{a}{p}$ or $\frac{b}{p}$. ($\because$ If a, b are integers and p is prime number then $\frac{ab}{p} \Rightarrow \frac{a}{p}$ or $\frac{b}{p}$)

$\Rightarrow a = 0$ or $b = 0$.

$\therefore I_p$ is without zero divisors.

$\therefore (I_p, +_p, \times_p)$ is an ID.

(VII) Let $s \neq 0 \in I_p$ then $1 \le s \le p-1 < p$.

Consider the following $(p-1)$ products.

$1 \times_p s,\ 2 \times_p s, \cdots\cdots (p-1) \times_p s$.

All these are elements of I_p by closure prop.

Also these elements are distinct.

because:

Let i, j be two integers such that

$1 \le i \le (p-1)$, $1 \le j \le (p-1)$ and $i > j$.

$\therefore 0 < (i-j) < p-1$

Now if possible that, $i \times_p s = j \times_p s$.

$\Rightarrow$ is and js leave the same remainder when each is divided by p.

$\Rightarrow (i-j)s$ is divided by p.

$\Rightarrow \frac{i-j}{p}$ or $\frac{s}{p}$

which is contradiction.

$\therefore i \times_p s \neq j \times_p s$

$\therefore 1 \times_p s, 2 \times_p s, \ldots \ldots (p-1) \times_p s$ are all distinct

One of these elements must be equal to 1.

Let $s' \times_p s = 1$

$\Rightarrow s'$ is the inverse of s.

i.e, each non-zero element of I_p has inverse.

$\therefore$ Inverse is satisfied w.r.t $\times$?.

$\therefore (I_p, +_p, \times_p)$ is a field.

Note: If 'p' is not prime then this is not a field. (Because this ring has zero divisors as well as every non-zero element doesnot posses the inverse.)

→ Prove that the set of residue classes modulo 'p' is a commutative ring with respect to $+^n$ and $\times^n$ of residue classes. Further show that the ring of residue classes modulo 'p' is a field iff 'p' is a prime.

Sol^n: Let Z_p be the set of residue classes modulo p. Then the set Z_p has distinct elements.

Let $Z_p = \{\bar{0}, \bar{1}, \bar{2}, \ldots \ldots \overline{(p-1)}\}$

(I) (i) Closure prop:

$\forall\ \bar{a}, \bar{b} \in Z_p$

$\Rightarrow \bar{a} + \bar{b} = \overline{a+b} \in Z_p$

$\therefore Z_p$ is closed w.r.t $+^n$.

$\because \overline{a+b} = \bar{r}$ where r is the remainder when $a+b$ is divided by p clearly $0 \le r < p$.

(ii) Asso. prop:

$\forall\ \bar{a}, \bar{b}, \bar{c} \in Z_p$.

$\Rightarrow (\bar{a}+\bar{b}) + \bar{c} = \overline{(a+b)} + \bar{c}$

$= \overline{(a+b)+c}$

$= \overline{a+(b+c)}$ ($\because +^n$ of integers is asso.)

$= \bar{a} + \overline{(b+c)}$

$= \bar{a} + (\bar{b}+\bar{c})$.

(iii) Existence of additive identity:

$\exists\ \bar{0} \in Z_p$ such that $\bar{0} + \bar{a} = \bar{a} = \bar{a} + \bar{0}$ $\forall\ \bar{a} \in Z_p$.

Since $\bar{0} + \bar{a} = \overline{0+a}$

$= \bar{a}$

and $\bar{a} + \bar{0} = \overline{a+0} = \bar{a}$

$\therefore \bar{0}$ is the identity element in Z_p.

(iv) Existence of additive inverse:

Let $\bar{a} \in Z_p$ ~~then $-\bar{a} \in Z_p$~~

we have $(\bar{-a}) + \bar{a} = \overline{(-a)+a}$

$= \bar{0}$

Similarly $\bar{a}+(\overline{-a}) = \overline{a+(-a)} = \bar{0}$.

$\therefore (\overline{-a})+\bar{a} = \bar{a}+(\overline{-a}) = \bar{0}$.

$\therefore \overline{-a}$ is the inverse of $\bar{a}$ in I_p w.r.t $+^n$.

(v) Comm. prop. of $+^n$:

$\forall\, \bar{a},\bar{b} \in I_p \Rightarrow \bar{a}+\bar{b} = \overline{a+b}$
$= \overline{b+a}$ ($+^n$ of integers is comm.)
$= \bar{b}+\bar{a}$.

$\therefore (I_p, +)$ is an abelian group.

(II) (i) Closure prop. of $\times^n$:

$\forall\, \bar{a},\bar{b} \in I_p \Rightarrow \bar{a}\cdot\bar{b} = \overline{a\cdot b} \in I_p$.

$\therefore I_p$ is closed w.r.t $\times^n$.

(ii) Asso. prop. of $\times^n$:

$\forall\, \bar{a},\bar{b},\bar{c} \in I_p$.

$$\Rightarrow (\bar{a}\cdot\bar{b})\,\bar{c} = (\overline{ab})\,\bar{c} = \overline{(ab)c} = \overline{a(bc)} = \bar{a}\,(\overline{bc}) = \bar{a}\cdot(\bar{b}\cdot\bar{c})$$

$\therefore (I_p, \cdot)$ is a semi group.

(III) Distributive Laws:

$$\forall\, \bar{a},\bar{b},\bar{c} \in I_p \Rightarrow \bar{a}\cdot(\bar{b}+\bar{c}) = \bar{a}\cdot(\overline{b+c}) = \overline{a(b+c)}$$
$= \overline{ab+ac}$ ($\because \times^n$ is distributive w.r.t $+^n$ in I)
$= \overline{ab}+\overline{ac}$
$= \bar{a}\,\bar{b}+\bar{a}\,\bar{c}$. (LDL)

Similarly $(\overline{b+c})\cdot\bar{a} = \overline{ba} + \bar{c}\cdot\bar{a}$

$\therefore (I_p, +, \cdot)$ is a ring.

(iv) Comm. prop of $\times^n$:

$\forall\ \bar{a}, \bar{b} \in I_p$

$\Rightarrow \bar{a}\cdot\bar{b} = \overline{ab}$
$= \overline{ba}$ ($\because$ $\times^n$ in integers is comm.)
$= \bar{b}\,\bar{a}$.

$\therefore (I_p, +, \cdot)$ is a commutative ring.

$\therefore (I_p, +, \cdot)$ is a finite comm. ring and

- it contains p elements.

Now suppose p is prime number.

we have to prove that I_p is a field.

(v) Let $\bar{a}, \bar{b} \in I_p$.

then $\bar{a}\cdot\bar{b} = 0$

$\Rightarrow \overline{a\cdot b} = 0$

$\Rightarrow p$ is divisor of ab. i.e, p/ab $\left(\text{or } \frac{ab}{p}\right)$

$\Rightarrow \frac{a}{p}$ or $\frac{b}{p}$. ($\because a, b \in \mathbb{Z}$ and p is prime then $\frac{ab}{p} \Rightarrow \frac{a}{p}$ or $\frac{b}{p}$)

$\Rightarrow \bar{a} = 0$ or $\bar{b} = 0$

$\therefore I_p$ is without zero divisors.

$\therefore I_p$ is a commutative ring without zero divisors. and I_p is finite

But every finite commutative ring without zero divisors is a field.

$\therefore I_p$ is a field.

Conversely, suppose that I_p is a field.

$\therefore I_p$ is an ID.

$\therefore I_p$ is without zero divisors.

Now we are to prove that p is prime number.

If possible suppose that 'p' is not prime number

then p is composite number.

Let $p = mn$ where $1 < m < p$, & $1 < n < p$.

$\Rightarrow \bar{p} = \overline{mn}$

$\Rightarrow \overline{mn} = \bar{p}$

$\Rightarrow \bar{m}\bar{n} = \bar{p}$

$\Rightarrow \bar{m}.\bar{n} = \bar{0}$ $(\because \bar{p} = \bar{0})$

Also $\bar{m} \neq \bar{0}$, $(\because 1 < m < p)$

Similarly $\bar{n} \neq \bar{0}$. $(\because 1 < n < p)$

$\therefore \bar{m}.\bar{n} = \bar{0}$

$\Rightarrow$ neither $\bar{m} = \bar{0}$ nor $\bar{n} = \bar{0}$.

Z_p has zero divisors which is contradiction.

$\therefore p$ is prime.

Note: The collection of residue classes mod p is not a field if p is composite number.

$\rightarrow F = \{0, 2, 4, 6, 8\} \pmod{10}$

$\rightarrow F = \{0, 1, 3, 5, 7, 8\} \pmod{11}$

$\rightarrow F = \{0, 1, 3, 4, 5, 9\} \pmod{11}$

2004. Prove that the ring Z_p or Z_p or $I/(p)$ of integers mod p is a field iff p is prime.

Proof: Let Z_p be a field.

$\therefore I_p$ is an ID $\Rightarrow I_p$ is without zero divisors.

To prove that p is prime.

if possible let p be not prime,

Then p is composite number.

Let $p = mn$ where $1 < m < p$, $1 < n < p$; $m, n \in I$.

$\Rightarrow mn = p$

$\Rightarrow mn \equiv 0 \pmod p$ $\quad (\because p \equiv 0 \pmod p)$.

$\Rightarrow mn = 0$ in I_p where $m \neq 0, n \neq 0$.

$(\because 1 < m < p, 1 < n < p.)$

$\therefore m \neq 0, n \neq 0 \in I_p \Rightarrow mn = 0$

$\therefore I_p$ has zero divisors.

which is contradiction.

$\therefore p$ is prime.

Conversely, suppose that p is a prime number.

we are to prove that I_p is a field.

W.K.T I_p is a finite comm. ring with unity p elements.

Now we have to show that I_p has no zero divisors.

Let $m, n \in I_p$. such that $mn = 0$ in I_p.

Then $\frac{mn}{p} \Rightarrow \frac{m}{p}$ or $\frac{n}{p}$ $\quad (\because p$ is prime$)$

$\Rightarrow m = 0$ or $n = 0$ in I_p.

$\therefore mn = 0$ in $I_p \Rightarrow m = 0$ or $n = 0$ in I_p

I_p has no zero divisors.

$\because I_p$ is a finite comm. ring without zero divisors.

$\therefore I_p$ is a field.

$\because I_p$ has no zero divisors.

$\because I_p$ is a finite comm. ring without zero divisors.

$\therefore I_p$ is a field.

Note: $I_2 = \{0, 1\}$, $I_3 = \{0, 1, 2\}$, $I_5 = \{0, 1, 2, 3, 4\}$ etc are all fields (finite).

INSTITUTE FOR IAS/IFoS EXAMINATIONS
NEW DELHI-110009
Mob: 09999197625

~~Def~~ Boolean Ring:

→ Let R be a ring. If for $a \in R$, we have $a^2 = a$ then a is an idempotent element.

→ A ring R is said to be a Boolean ring if for every element of it is an Idempotent element.

i.e. In a ring R, if $a^2 = a \ \forall a \in R$ then R is called a Boolean ring.

124 / 20 of 4 → ~~Theorem: If R is Boolean ring then (i) $a+a=0 \ \forall a \in R$~~

(ii) $a+b=0 \Rightarrow a=b$ and (iii) R is commutative under $\times$?

Proof: Given that R is Boolean ring.

$\forall a \in R \Rightarrow a+a \in R$

Since $a^2 = a \ \forall a \in R$.

we have

$(a+a)^2 = a+a$

$\Rightarrow (a+a)(a+a) = a+a$

$\Rightarrow a(a+a) + a(a+a) = a+a$

$\Rightarrow (a^2+a^2) + (a^2+a^2) = a+a$ $\cancel{(\because a^2 = a \ \forall a \in R)}$

$\Rightarrow (a+a) + (a+a) = (a+a)$ ~~+0~~ $\cancel{(\because a^2 = a)}$

$\Rightarrow (a+a) + (a+a) = (a+a) + 0$

$\Rightarrow a+a = 0$ (By LCL)

(ii) For $a, b \in R$, $a+b=0$

$\Rightarrow a+b = a+a$ ($\because a+a=0$ i.e. by (i))

$\Rightarrow b = a$ (By LCL)

$\Rightarrow a = b$

(iii) $a, b \in R \Rightarrow a+b \in R$

$\Rightarrow (a+b)^2 = a+b$

$\Rightarrow \cancel{(a+b)(a+b) = a+b}$

$\Rightarrow a(a+b) + b(a+b) = a+b$

$\Rightarrow (a^2+ab) + (ba+b^2) = a+b$

$\Rightarrow a+(ab+ba)+b = a+b$

$\Rightarrow (a+b)+(ab+ba) = a+b$

$\Rightarrow (a+b)+(ab+ba) = (a+b)+0$

$\Rightarrow ab+ba=0$ (by LCL)

$\Rightarrow ab=ba$ (by (ii))

Note: The above theorem can be stated as follows.

"every Boolean ring is abelian".

→ If $a \neq 0$ is an idempotent element of an ID then $a=1$.

Sol^n: Let $(R,+,\cdot)$ be an ID.

$a \neq 0 \in R$ is an idempotent element.

$\therefore a^2 = a$

$\Rightarrow a^2 = a\cdot 1$ $(\because a\cdot 1 = a)$

$\Rightarrow a^2 - a\cdot 1 = 0$

$\Rightarrow a(a-1)=0$

$\Rightarrow a-1=0$ ($\because$ R has no zero divisors) & $a \neq 0$

$\Rightarrow a=1$

Note: [1]. An ID contains only two idempotent elements 0 & 1.

[2]. The only idempotent elements in a field are 0 & 1.

Nilpotent Element:

Let R be a ring and $a \in R$. If there exists $n \in N$ ~~such~~ that $a^n=0$ then 'a' is called nilpotent element of R.

Note: 0 is always nilpotent element of ring R.

Theorem An ID has no nilpotent other than zero.

Soln: Let R be an ID and $a \neq 0 \in R$.

we have $a^1 = a \neq 0$, $a^2 = a \cdot a \neq 0$
($\because R$ has no zero divisors)

Let $a^n \neq 0$ for $n \in N$

then $a^{n+1} = a^n \cdot a \neq 0$ ($\because R$ has no zero divisors)

$\therefore$ By induction $a^n \neq 0$ $\forall n \in N$.

$\therefore a \neq 0 \in R$ is not a nilpotent element.

Examples:-

(1) In the ring R_2 of all 2×2 matrices over integers.

$\begin{pmatrix}1&0\\1&0\end{pmatrix}$, $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ are idempotent.

Since $\begin{pmatrix}1&0\\1&0\end{pmatrix}\begin{pmatrix}1&0\\1&0\end{pmatrix} = \begin{pmatrix}1&0\\1&0\end{pmatrix}$,

$\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix} = \begin{pmatrix}1&0\\0&0\end{pmatrix}$ etc.

and $\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix}$ are nilpotent elements

since $\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$;

$\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$.

(2) In the ring $Z_4 = \{0,1,2,3\}$ of integers mod 4;
0 and 1 are the only idempotent elements and
0 & 2 are the only nilpotent elements.
($\because 2^2 = 0$ in Z_4)

(3) In the ring $Z_{10} = \{0,1,2,3,4,5,6,7,8,9\}$ of integers modulo 10;
0, 1, 5, 6 are the idempotent elements.
and 0 is the only nilpotent element.

(4) If a, b are nilpotent elements in a commutative ring R then $a+b$, $a \cdot b$ are nilpotent elements.

(5) In a ring R, a non-zero idempotent element cannot be nilpotent.

(6) If a, b are nilpotent elements in a non-commutative ring R then $a+b$, $a \cdot b$ are not nilpotent elements.

Ex: The ring M_2 of all 2×2 matrices over the integers is non-commutative.

where $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ are nilpotent (Since $A^2 = B^2 = 0$)

$A+B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not nilpotent.

Since $(A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$(A+B)^3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ so on.

we get $(A+B)^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\forall n \in N$.

and $A \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ is not nilpotent.

Since $(AB)^2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$; $(AB)^3 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ and so on.

we get $(AB)^n = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ $\forall n \in N$.

→ Let R be a commutative ring and $a \in R$ if a is nilpotent then ab is nilpotent for each $b \in R$.

Soln: Since a is nilpotent.

$\therefore a^n = 0$ for some $n \in N$.

Since R is commutative.

$\therefore (ab)^n = a^n \cdot b^n \quad \forall a, b \in R$.

$= 0 \cdot b^n$

$= 0$

$\therefore ab$ is nilpotent $\forall b \in R$.

→ Let R be ring and $a, b \in R$ if ab is nilpotent then ba is nilpotent.

Sol: Since ab is nilpotent.

$\therefore (ab)^n = 0$ for some $n \in N$.

Now consider

$$(ba)^{n+1} = ba.ba \cdots ba.ba \quad (n+1 \text{ times})$$
$$= b(ab).(ab) \cdots (ab)\,a.$$
$$= b(ab)^n a$$
$$= b(0)a \quad (\because (ab)^n = 0)$$
$$= 0$$

$\therefore$ ba is nilpotent.

Problems:

→ The set of all 2×2 matrices over the ring $Z_2 = \{0,1\}$ of integers modulo 2 is a finite non-commutative ring.

Sol: Hint:

the ring S has $2^4 = 16$ elements.

$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix},$

$\begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&1\end{pmatrix}.$

→ The set $M = \left\{\begin{bmatrix}0&a\\0&b\end{bmatrix} / a, b \in R\right\}$ is a non-commutative ring without unity under matrix + & matrix ×.

Note: $\begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&0\\0&0\end{pmatrix}$; $\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix}$

$\therefore \begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} \neq \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix}$.

→ If R is a ring with unity satisfying $(xy)^2 = x^2y^2 \; \forall x, y \in R$ then R is commutative.

Sol: We have $(xy)^2 = x^2y^2 \; \forall x, y \in R$ ——— ①

Replacing y by $y+1 \in R$ in ①, we get

$[x(y+1)]^2 = x^2(y+1)^2$

$\Rightarrow (xy+x)^2 = x^2(y^2+2y+1)$

$\Rightarrow (xy+x)(xy+x) = x^2(y^2+2y+1)$

$\Rightarrow (xy)^2 + (xy)x + x(xy) + x^2 = x^2y^2 + 2x^2y + x^2$ —— (2)

$\Rightarrow (xy)^2 + (xy)x + x(xy) + x^2 = (xy)^2 + 2x^2y + x^2$

$\Rightarrow (xy)x + x(xy) = 2x^2y \quad (\because \text{LCL \& RCL in } (R,+))$

$\Rightarrow xyx + x^2y = 2x^2y$

$\Rightarrow \cancel{xyx = x^2y \ \forall x,y \in R}$ — (3) (R.C.L)

Replacing x by $x+1 \in R$ in (3),

$(x+1)y(x+1) = (x+1)^2y$

$\Rightarrow (x+1)(yx+y) = (x+1)(xy+y)$.

$\Rightarrow xyx + xy + yx + y = x^2y + xy + xy + y$

$\Rightarrow yx = xy \quad \forall x,y \in R$

$(\because \text{LCL \& RCL in } (R,+))$

$\therefore R$ is a comm. ring.

→ Give an example of a non-commutative ring R without unity such that $(xy)^2 = x^2y^2 \ \forall x,y \in R$.

Sol: Consider the ring R of 2×2 matrices

$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \Big/ a,b \in \mathbb{Z} \right\}$.

Clearly, R is non-commutative.

Since $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$; $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

$\therefore \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ [Note: the possible unity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin R$]

Let $X = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$

then $XY = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$; $X^2 = \begin{pmatrix} a^2 & ab \\ 0 & 0 \end{pmatrix}$, $Y^2 = \begin{pmatrix} c^2 & cd \\ 0 & 0 \end{pmatrix}$

$(XY)^2 = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}\begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a^2c^2 & a^2cd \\ 0 & 0 \end{pmatrix} = X^2Y^2$.

→ A ring R is commutative iff $a^2-b^2=(a+b)(a-b)$ $\forall a,b \in R$.

Sol: Let R be commutative

Then $ab=ba$ $\forall a,b\in R$

R.H.S $(a+b)(a-b) = a(a-b)+b(a-b)$

$= a^2-ab+ba-b^2$

$= a^2-b^2$ $(\because ab=ba)$.

Conversely suppose that

$(a^2-b^2)=(a+b)(a-b)$

$\Rightarrow a^2-b^2 = a^2-ab+ba-b^2$ $(\because$ RCL & LCL in $(R,+))$

$\Rightarrow 0 = -ab+ba$

$\Rightarrow ab=ba.$ $\forall a,b\in R$

Hence R is a Commutative ring.

→ The set of all 2×2 matrices over the finite field $Z_3=\{0,1,2\}$ is a finite non-commutative ring of order $3^4=81$, under matrix addition and matrix multiplication.

→ The set of all 3×3 matrices over a finite field is a finite non-commutative ring under matrix $+^n$ and matrix $\times^n$.

(Hint: If a field having n elements then the required ring R has n^9 elements.)

further R is non-commutative.

Since $AB\neq BA$; where $A=\begin{pmatrix}0&0&0\\1&0&0\\0&0&0\end{pmatrix}$ $B=\begin{pmatrix}0&0&1\\0&0&0\\0&0&0\end{pmatrix}$

→ Let $(R,+,\cdot)$ be a ring. Then the system $(R,+,o)$ is also a ring where $xoy=y\cdot x$ $\forall x,y\in R$.

Note: The ring $(R,+,o)$ is called the opposite ring of R written as R^{op}.

Subrings

Defn: Let R be a ring. S be a non-empty subset of R (i.e., $S \subseteq R$), if S is a ring w.r.t binary operations defined in R then S is called a subring of R.

Note: [1] If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ then $(S,+)$ is a subgroup of the group $(R,+)$.

Defn: Let $(F,+,\cdot)$ be a field and $(S,+,\cdot)$ be a subring of F. If $(S,+,\cdot)$ is a field then we say that 'S' is a subfield of F.

(Or)

Let F be a field and S is a non-empty subset of F. If S is field w.r.t binary operations defined in F then S is called a subfield of F.

Note: [1] If $(S,+,\cdot)$ is subfield of $(F,+,\cdot)$ then

a) $(S,+)$ is a subgroup of $(F,+)$.

b) $(S-\{0\},\cdot)$ is a subgroup of $(F-\{0\},\cdot)$

[2] If $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$, then

a) $(S,+)$ is a subgroup of $(R,+)$

b) $(S,\cdot)$ is a subsemigroup of $(R,\cdot)$

and c) Distributive laws hold.

Examples:

→ The set of even integers is a subring of the ring of integers under "+" and "×".

→ $(Z,+,\cdot)$, $(Q,+,\cdot)$ are subrings of the ring of real numbers $(R,+,\cdot)$.

→ Let $(Q,+,\cdot)$ be the ring of rational numbers.

If $S=\{\frac{a}{2} / a\in\mathbb{Z}\}$ then S is a non-empty subset of Q and $(S,+)$ is a subgroup of $(Q,+)$.

but for $\frac{1}{2}\in S$

we have

$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}\notin S.$

$\therefore$ x^n is not a b-o on S.

$\therefore$ $(S,+,\cdot)$ is not a Subring of $(Q,+,\cdot)$

→ Let $(R,+,\cdot)$ be a ring. ~~and $0\in R$~~ then $S=\{0\}$ is a non-empty subset of R and $(S,+,\cdot)$ is itself a ring.

$\therefore$ $(S,+,\cdot)$ is a Subring of R.

$\therefore$ If R is any ring then $\{0\}$ and R itself are always subrings of R.

These are known as improper subrings of R.

Other rings, if any, of R called proper subrings of R.

Theorem. Let S be a non-empty subset of a ring R. Then S is a subring of R iff $\forall a,b\in S \Rightarrow a-b\in S$ and $ab\in S$.

proof: N.C :-

Let S be a subring of R.

By the defn 'S' is a ring w.r.t the b-o's of R.

(1) $\forall a,b\in S \Rightarrow a\in S, -b\in S$ (inverse prop. of S)

$\Rightarrow a+(-b)\in S$ (by closure prop)

$\Rightarrow a-b\in S.$

(2) $\forall a,b\in S \Rightarrow a\cdot b\in S$ (by closure prop. of S)

$\therefore \forall a,b\in S \Rightarrow a-b\in S$ & $ab\in S$.

S.C:- Let $S\subseteq R$.

$\forall a,b\in S \Rightarrow a-b\in S$ (1) & $ab\in S$ (2)

(I). (i) [illegible]

[illegible] $\subseteq R$ (by ①)

[illegible] $\in S \subseteq R$

$\therefore \forall a \in S \subseteq R \ \exists\, 0 \in S \subseteq R$ such that $0+a=a+0=a$

$\therefore 0$ is the identity element in S.

$\therefore$ Identity prop. is satisfied.

(ii) $0 \in S,\ a \in S \Rightarrow 0-a \in S$ (hyp ①)

$\Rightarrow -a \in S$

$\therefore \forall a \in S,\ \exists\, -a \in S$ such that $a+(-a)=(-a)+a=0$ (by inverse of R)

$\therefore$ Inverse prop is satisfied in S.

Inverse of a is $-a$ in S.

(iii) $\forall\, b \in S \Rightarrow -b \in S$

$\therefore \forall\, a, \cancel{-b \in S} \Rightarrow a-(-b) \in S$ (hyp)

$\Rightarrow a+b \in S$

$\therefore a, b \in S \Rightarrow a+b \in S$.

$\therefore$ Closure prop. in S is satisfied.

(iv) $\forall a, b, c \in S \subseteq R$.

$\Rightarrow a+(b+c)=(a+b)+c$ (by asso. prop. of R)

$\therefore$ Asso. property in S is satisfied.

(v) $a, b \in S \subseteq R \Rightarrow a+b=b+a$ (by comm. prop. of R)

$\therefore$ Comm. prop in S is satisfied.

$\therefore (S,+)$ is an abelian group.

(II) (i) $\forall a, b \in S \Rightarrow ab \in S$ (by hyp ②)

Closure prop. in S is satisfied.

(ii) $\forall\, a, b, c \in S \subseteq R \Rightarrow (ab)c = a(bc)$ (by asso. prop. of R)

$\therefore X^n$ is asso. in S.

$\therefore (S, \cdot)$ is a semigroup.

(III) $a, b, c \in S \subseteq R \Rightarrow a\cdot(b+c) = a\cdot b + a\cdot c$ | X^n is distributive w.r.t $+^n$ in R

& $(b+c)\cdot a = ba + ca$

II (i) ~~$a, a \in K \subseteq F$~~ $\Rightarrow a a^{-1} \in K$ (by ①)
$\Rightarrow e \in K$. (by inverse prop. of F)

$\therefore \forall$ ~~$a \in K$~~ $\subseteq F$, $\exists e \in K \subseteq F$ such that $a.e = e.a = a$. (by identity prop. in F)

$\therefore$ Identity prop. in K is satisfied.

and e is th identity element in k.

~~(ii) $e \in K \subseteq F$~~, $b \neq 0 \in K \subseteq F$.
$\Rightarrow e b^{-1} \in K \subseteq F$ (by hyp(ii))
$\Rightarrow b^{-1} \in K \subseteq F$

$\therefore b \neq 0 \in K \Rightarrow b^{-1} \in K$ such that $b b^{-1} = b^{-1} b = e$ (by inverse of F)

$\therefore$ inverse of b is b^{-1} in k.

$\therefore$ Inverse prop. is satisfied

(iii) $\forall b \neq 0 \in K \Rightarrow b^{-1} \in K$
$\therefore \forall a, b^{-1} \in K \subseteq F \Rightarrow a(b^{-1})^{-1} \in K$ (by ①)
$\Rightarrow ab \in K$
$\therefore$ K is closed w.r.t x^n.

(iv) $\forall a, b, c \in K \subseteq F \Rightarrow (ab)c = a(bc)$ (by asso prop in F)
$\therefore$ K is asso. under x^n

(v) $\forall a, b \in K \subseteq F \Rightarrow ab = ba$ (by comm. of F)
$\therefore$ comm. in K is satisfied w.r.t x^n.

(vi) $\forall a, b, c \in K \subseteq F \Rightarrow a \cdot (b+c) = ab + ac$ & $(b+c)a = ba + ca$ } x^n is distributive w.r.t $+^n$ in F

$\therefore$ Distributive laws are satisfied

$\therefore$ Distributive laws are satisfied.

$\therefore$ $(S,+,\cdot)$ is a ring.

$(S,+,\cdot)$ is a subring of $(R,+,\cdot)$

Note:

Let R be a ring and S is a non-empty subset of R.

S is a subring of R iff (i) $S+(-S)=S$
(ii) $SS \subseteq S$.

Theorem

Let F be a field. Let K be a non-empty subset of F. Then K is a subfield of F iff

$\forall a,b \in K \Rightarrow a-b \in K$ & $ab^{-1} \in K$.

proof

N.C:

Let K be a subfield of F, Then by defn, K is a field w.r.t. b-o's defined in F.

(i) $\forall a,b \in K \Rightarrow a \in K, -b \in K$ (by inverse of K)

$\Rightarrow a+(-b) \in K$ (by Closure of K)

$\Rightarrow a-b \in K$

(ii) $b \neq 0 \in K \Rightarrow b^{-1}$ exists in K. ($\because$ x^{ve} inverse in K)

$\therefore \forall a \in K, b^{-1} \in K \Rightarrow ab^{-1} \in K$ (By closure prop. of K)

S.C:

$K \subseteq F$.

Let $a,b \in K \Rightarrow a-b \in K$ & $ab^{-1} \in K$.

(I) To show $(K,+)$ is an abelian group.

$\therefore (K,+,\cdot)$ is a field.

$\therefore (K,+,\cdot)$ is a subfield of $(F,+,\cdot)$

Examples:

$\rightarrow$ P.T $S_1 = \{\bar{0}, \bar{3}\}$, $S_2 = \{\bar{0}, \bar{2}, \bar{4}\}$ are subrings of $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ w.r.t $+^n$ & $\times^n$ of residue classes.

Sol^n: Since $(Z_6,+,\cdot)$ is a ring.

from the additive inverse of Z_6: $-\bar{0}=\bar{0}$, $-\bar{2}=\bar{4}$, $-\bar{3}=\bar{3}$, $-\bar{3}=\bar{4}$, $-\bar{1}=\bar{5}$.

and $S_1 = \{\bar{0}, \bar{3}\} \subseteq Z_6$.

$+$	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	0

$\cdot$	$\bar{0}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{3}$	$\bar{0}$	$\bar{3}$

From the above tables

$\forall \bar{a}, \bar{b} \in S_1 \Rightarrow \bar{a} - \bar{b} \in S_1$

Since $\bar{0}, \bar{3} \in S_1$

$\Rightarrow \bar{0} - \bar{3} = \overline{0-3}$

$= -\bar{3} \in S_1$

$= \bar{3} \in S_1$ etc.

and $\bar{a}, \bar{b} \Rightarrow \bar{a}\,\bar{b} \in S_1$

Since $\bar{0}, \bar{3} \in S_1 \Rightarrow \bar{0}\cdot\bar{3} = \bar{0} \in S_1$ etc

$\therefore S_1$ is a subring of Z_6.

Now $S_2 = \{\bar{0}, \bar{2}, \bar{4}\} \subseteq Z_6$

$+$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$

From the above tables

$\forall \bar{a}, \bar{b} \in S_2 \Rightarrow \bar{a} - \bar{b} \in S_2$

Since $\bar{0}, \bar{2} \Rightarrow \bar{0} - \bar{2} = \overline{0-2}$

$= \overline{-2}$

$= \bar{4} \in S_2$ etc.

$\forall \bar{a}, \bar{b} \in S_2 \Rightarrow \bar{a}\cdot\bar{b} \in S_2$

since $\bar{0}, \bar{2} \in S_2 \Rightarrow \bar{0}\cdot\bar{2} = \bar{0} \in S_2$.

$\therefore$ S_2 is a subring of Z_6.

Now we see that $S_1 \cap S_2 = \{\bar{0}\}$ is a trivial subring of Z_6.

But $S_1 \cup S_2 = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$ is not a subring of Z_6

because $\bar{2}, \bar{3} \in S_1 \cup S_2 \Rightarrow \bar{2}+\bar{3} = \bar{5} \notin S_1 \cup S_2$

Theorem The intersection of two subrings of a ring R is a subring of R.

proof: Let S_1 & S_2 are two subrings of a ring R.

Let $S = S_1 \cap S_2$

$a, b \in S \Rightarrow a, b \in S_1 \cap S_2$.

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

$\Rightarrow a-b \in S_1$ and $a-b \in S_2$ ($\because S_1$ & S_2 are
$ab \in S_1$ $\quad ab \in S_2$. two subrings of R)

$\Rightarrow a-b \in S_1 \cap S_2$ and $ab \in S_1 \cap S_2$

i.e., $a-b \in S$, $ab \in S$.

$\therefore$ $S_1 \cap S_2$ is a subring of R.

Theorem Intersection of arbitrary number of subrings a subring of R.

proof: Let $S_1, S_2, \ldots\ldots S_n$ are subrings of R.

Let $S = S_1 \cap S_2 \cap \ldots\ldots \cap S_n \ldots\ldots$

$= \bigcap_{i \in N} S_i$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2 \cap, \ldots\ldots$

$\Rightarrow a, b \in \bigcap_{i \in N} S_i$

$\Rightarrow a, b \in S_i \quad \forall i \in N$

$\Rightarrow a-b \in S_i$ and $ab \in S_i \ \forall i \in N$. ($\because S_i$ is a subring).

$\Rightarrow a-b \in \bigcap_{i\in N} S_i$ & $ab \in \bigcap_{i \in N} S_i$

$\Rightarrow a-b \in S$ & $ab \in S$

$\therefore S_1 \cap S_2 \cap \dots \cap S_n \dots$ is a subring of R.

$\therefore$ Intersection of arbitrary no. of subrings is a subring.

Theorem: Union of two subrings of R need not be a subring of R.

Soln: Let $R = I$ (ie the ring of integers)

Let $S_1 = \{2n / n \in I\}$

$= \{\dots -6, -4, -2, 0, 2, 4, 6, \dots\}$

$S_2 = \{3n / n \in I\}$

$= \{\dots -9, -6, -3, 0, 3, 6, 9, \dots\}$ be two subrings of R.

$2 \in S_1,\ 3 \in S_2 \Rightarrow 2, 3 \in S_1 \cup S_2$

$\Rightarrow 2+3 = 5 \notin S_1 \cup S_2$

$\therefore S_1 \cup S_2$ is not closed under $+^n$.

$\therefore S_1 \cup S_2$ is not a subring of R.

Theorem: If S_1 and S_2 are two subrings of a ring R then $S_1 \cup S_2$ is a subring of R iff $S_1 \subset S_2$ or $S_2 \subset S_1$

proof: Let $S_1 \cup S_2$ be a subring of R.

Now we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$

If possible suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$

Since $S_1 \not\subset S_2$

Let $a \in S_1$ but $a \notin S_2$.

Since $S_2 \not\subset S_1$

Let $b \in S_2$ but $b \notin S_1$

Now we have

$a \in S_1, b \in S_2 \Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a+b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is ring)

$\Rightarrow a+b \in S_1$ or $a+b \in S_2$

Now we have

$a \in S_1, a+b \in S_1$

$\Rightarrow (a+b)-a \in S_1$ ($\because S_1$ is subring of R)

$\Rightarrow b \in S_1$

which is contradiction.

Now we have

$b \in S_2, a+b \in S_2$

$\Rightarrow (a+b)-b \in S_2$ ($\because S_2$ is subring of R)

$\Rightarrow a \in S_2$

which is contradiction.

$\therefore$ Our assumption that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$ is wrong.

$\therefore S_1 \subset S_2$ or $S_2 \subset S_1$

Conversely suppose that $S_1 \subset S_2$ or $S_2 \subset S_1$

prove that $S_1 \cup S_2$ is a subring

Since $S_1 \subset S_2 \Rightarrow S_1 \cup S_2 = S_2$

$\therefore S_1 \cup S_2$ is a subring of R.

($\because S_2$ is subring of R)

Since $S_2 \subset S_1 \Rightarrow S_1 \cup S_2 = S_1$

$\therefore S_1 \cup S_2$ is a subring of R.

($\because S_1$ is subring of R)

→ The centre of a ring R is a subring of R.

Sol^n: Let $Z(R)$ be the centre of Ring R then

$Z(R) = \{a \in R \mid xa = ax \ \forall x \in R\}$

Clearly $Z(R)$ is non-empty.

Since $0x = x0 \ \forall x \in R$

$\Rightarrow 0 \in Z(R)$

Let $a, b \in Z(R)$

where $xa = ax$; $xb = bx \ \forall x \in R$ —— (1)

Now $(a-b)x = ax - bx$

$= xa - xb$

$= x(a-b)$

$\therefore (a-b)x = x(a-b) \ \forall x \in R$

$\therefore a-b \in Z(R)$

Now $(ab)x = a(bx)$

$= a(xb)$ (by (1))

$= (ax)b$

$= (xa)b$ (by (1))

$= x(ab)$

$\therefore (ab)x = x(ab) \ \forall x \in R$.

$\therefore ab \in Z(R)$

$\therefore Z(R)$ is a subring of R.

→ The centre of a division ring is a field.

Sol^n: Let $Z(R)$ be the centre of the division ring R.

then $Z(R) = \{a \in R / xa = ax \ \forall x \in R\}$ —— (1)

Now we shall show that $Z(R)$ is a field

W.K.T $Z(R)$ is a subring of R.

$\therefore Z(R)$ is a ring

Let $a, b \in Z(R)$

then $ax = xa$, $\forall x \in R$

In particular $ab = ba$ $\forall a, b \in Z(R)$

$\therefore Z(R)$ is a commutative ring.

Since R is division ring,

$\because 1 \in R$ and $1 \cdot x = x \cdot 1 = x \quad \forall x \in R$

$\therefore 1 \in Z(R)$

$\therefore Z(R)$ has unity.

Finally we show that each non-zero element of $Z(R)$ has a multiplicative inverse in $Z(R)$.

Let $a \neq 0 \in Z(R)$ then $a \neq 0 \in R$

$\Rightarrow a^{-1} \in R$ exists ($\because R$ is a division ring)

Let $x \neq 0 \in R$ then $x^{-1} \in R$ exists.

we have $xa^{-1} = (ax^{-1})^{-1}$

$= (x^{-1}a)^{-1}$ $\left(\because a \in Z(R) \Rightarrow ax^{-1} = x^{-1}a\right)$

$= a^{-1}x$.

$\therefore xa^{-1} = a^{-1}x \quad \forall x \in R$.

and $0a^{-1} = a^{-1}0$

$\therefore a^{-1}x = xa^{-1} \quad \forall x \in R$.

$\therefore a^{-1} \in Z(R) \quad \forall a \in Z(R)$

$\therefore Z(R)$ is a field.

→ ~~Show by means of~~ an example that a subring of a ring with unity may fail to be a ring with unity.

Ex: The ring I of integers is a ring with unity. But the set E of even integers is a subring of I without unity.

→ The subring of a non-commutative ring may or may not commutative.

Sol: The ring M_2 of 2×2 matrices over integers is non-commutative.

Since $\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} = \begin{pmatrix}1&1\\1&0\end{pmatrix}$; $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix} = \begin{pmatrix}0&1\\1&1\end{pmatrix}$

$$\therefore \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} \neq \begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

The set $S = \left\{ \begin{pmatrix}a&0\\0&0\end{pmatrix} / a \in \mathbb{Z} \right\}$ is a subring of M_2 which is commutative.

Since $\begin{pmatrix}a&0\\0&0\end{pmatrix}\begin{pmatrix}b&0\\0&0\end{pmatrix} = \begin{pmatrix}ab&0\\0&0\end{pmatrix}$

$$= \begin{pmatrix}b&0\\0&0\end{pmatrix}\begin{pmatrix}a&0\\0&0\end{pmatrix}$$

→ (i) Ring which is not commutative but has a subring which is commutative.

(ii) Ring which has no unity but subring which has unity.

Sol (ii) $R = \left\{ \begin{bmatrix}a&b\\0&0\end{bmatrix} / a, b \in \mathbb{Z} \right\}$ is a ring which has no unity.

(Note: the possible unity $\begin{pmatrix}1&0\\0&1\end{pmatrix} \notin R$)

It can be verified that none of $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $\begin{pmatrix}1&1\\0&0\end{pmatrix}$ unity of R.

However, $S = \left\{ \begin{pmatrix}a&0\\0&0\end{pmatrix} / a \in \mathbb{Z} \right\}$ is a subring of R, which has $\begin{pmatrix}1&0\\0&0\end{pmatrix}$ as the unity of S.

→ Show that $S = \{0, 2, 4, 6, 8\}$ is a subring of $\mathbb{Z}_{10}$ with unity different from that $\mathbb{Z}_{10}$, the ring of integers mod 10.

Sol:

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\times_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

From the above tables:

$\forall a, b \in S \Rightarrow a-b \in S$ and $a \times b \in S$.

Since $0, 4 \in S \Rightarrow 0-4 = -4 = 6 \in S$ etc.

and $0 \times 4 = 0 \in S$ etc.

$\therefore$ S is a subring of Z_{10} where the unity is 6.

→ The sum of two subrings of a ring need not be a subring.

Ex:- Let $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\}$; $T = \left\{ \begin{bmatrix} 0 & c \\ 0 & 0 \end{bmatrix} / c \in Z \right\}$ be two subrings of ring M_2 of 2×2 matrices over integers.

~~Now the sum of S & T is~~ $\cancel{S+T = \left\{ \begin{pmatrix} a & c \\ b & 0 \end{pmatrix} / a, b, c \in Z \right\}}$

Let $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 2 \\ 2 & 0 \end{bmatrix} \in S+T$.

but $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 2 & 2 \end{pmatrix} \notin S+T$

$\therefore$ S+T is not a subring of M_2.

→ Let R be the ring of 2×2 matrices over reals. then $S = \left\{ \begin{bmatrix} x & x \\ x & x \end{bmatrix} / x \in \mathbb{R} \right\}$ is a subring of R and has a unity different from the unity of R.

Sol:

~~Let~~ $\cancel{A = \begin{pmatrix} x & x \\ x & x \end{pmatrix}}$, $B = \begin{pmatrix} y & y \\ y & y \end{pmatrix} \in S$; $x, y \in \mathbb{R}$

then $A-B = \begin{pmatrix} x-y & x-y \\ x-y & x-y \end{pmatrix} \in S$ $\left(\because x, y \in \mathbb{R} \Rightarrow x-y \in \mathbb{R} \right)$

and $AB = \begin{pmatrix} 2xy & 2xy \\ 2xy & 2xy \end{pmatrix} \in S$ $(\because xy \in \mathbb{R})$

$\therefore$ S is a subring of R.

Here the unity of S is $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$

and the unity of R is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Problems:

→ Show that the set $S = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \middle/ a, b \in Z \right\}$ is a subring of the ring M_2 of 2×2 matrices over integers.

Solⁿ: Clearly S is a non-empty subset of M_2 $\left(\because \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S\right)$

Let $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \in S$ and $B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} \in S$ where $a, b, c, d \in Z$

Then $A - B = \begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in S$ $(\because a-c, b-d \in Z)$

and $A \cdot B = \begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in S$ $(\because ac, bc \in Z)$

$\therefore S$ is a subring of the ring of 2×2 matrices over integers.

H.W. → Show that the set of matrices $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ is a subring of the ring of 2×2 matrices with integral elements.

→ Let R be the ring of integers. Let m be any fixed integer and let 'S' be any subset of R such that

$S = \{ \dots \dots -3m, -2m, -m, 0, m, 2m, \dots \dots \}$

Then S is a subring of R.

Solⁿ: Let $S = \{ rm / r \in I,\ m \text{ is fixed integer} \}$.

Clearly S is non-empty subset of R. $(\because \{0\} \subseteq R)$

Let $a = rm$, $b = sm$ be two elements of S, $r, s \in I$.

we have

$a - b = rm - sm$

$= (r-s)m \in S$ $(\because r-s \in I)$

and $ab = (rm)(sm)$

$= (rsm)m \in S$ $(\because rsm \in I)$

$\therefore S$ is a subring of R.

→ If 'a' is a fixed element of a ring R, show that $I_a = \{ x \in R / ax = 0 \}$ is a subring of R.

Sol^n: Since $a0 = 0$

$\therefore 0 \in I_a$

$\Rightarrow I_a$ is a non-empty subset of R

Let $x, y \in I_a$ then $ax = 0$ & $ay = 0$

Now $a(x-y) = ax - ay$
$= 0 - 0$
$= 0$

$\therefore x - y \in I_a$

Again $a(xy) = (ax)y$
$= 0y$
$= 0$

$\therefore xy \in I_a$

$\therefore I_a$ is a subring of R.

Characteristic of a ring:

→ A ring R is said to be of finite characteristic, if there exists a +ve integer 'n' such that $na = 0$ for all $a \in R$.

→ If a ring R is of finite characteristic, then the characteristic ~~of R~~ is defined as the smallest +ve integer 'p' such that $pa = 0 \ \forall a \in R$. We write it as $\text{Char } R = p$.

→ A ring R is said to be of characteristic zero or infinite if there exists no +ve integer 'n' such that $na = 0 \ \forall a \in R$.

Examples:

→ $\text{Char } \mathbb{Z} = 0$, $\text{Char } \mathbb{Q} = 0$, $\text{Char } \mathbb{R} = 0$

→ $\text{Char } \mathbb{Z}_2 = 2$ where $\mathbb{Z}_2 = \{0, 1\}$

Since $1 \times_2 0 = 0$ $\quad 1 \times_2 1 = 1$
$2 \times_2 0 = 0$ $\quad 2 \times_2 1 = 0$
$3 \times_2 1 = 1$
$4 \times_2 1 = 0$

Here 2 is the smallest +ve integer such that
$2 \times_2 0 = 0$ & $2 \times_2 1 = 0$.

→ Char $Z_3 = 3$, where $Z_3 = \{0, 1, 2\}$.

In general Char $Z_n = n$.
where $Z_n = \{0, 1, 2, 3, \cdots (n-1)\}$
is the ring of integers modulo 'n'.

Theorem If R is a ring with unity element, then R has characteristic $p > 0$ iff p is the least +ve integer such that $p1 = 0$.

proof: Let the Char. of the ring $R = p$. $(p > 0)$.

By defn $pa = 0 \ \forall a \in R$
where p is the least +ve integer.

In particular, $p1 = 0$

Conversely suppose that p is the least +ve integer such that $p1 = 0$

Now for any $a \in R$, we have

$$pa = a + a + \cdots + a \ (p \text{ times})$$
$$= a(1 + 1 + \cdots + 1 \ (p \text{ times}))$$
$$= a(p1)$$
$$= a(0) \quad (\because p1 = 0 \text{ where } p \text{ is the least +ve integer})$$

$\therefore pa = 0 \ \forall a \in R$
where p is the least +ve integer.

$\therefore$ Char. of the ring $R = p$.

Theorem If any element of a ring R is of order zero when regarded as an element of $(R, +)$ group then characteristic of R is zero.

proof: Let $a \in R$
When 'a' is considered as an element of the group $(R, +)$

Let $O(a)=0$ i.e, order of $a=0$.
By the defn of the order of an element of a group there exists no +ve integer 'n' such that $na=0$

$\therefore$ Char. of $R=0$

Theorem → The Characteristic of a ring with unit element is the order of the unit element regarded as a member of the additive group.

proof:
~~Let $(R,+,\cdot)$ be a ring.~~
So that $(R,+)$ is its additive group.

Case(i): Let $O(1)=0$ when the unit element 1 is regarded as an element of $(R,+)$
By the defn of order of an element in a group, there exists no +ve integer 'n' such that $n\cdot 1=0$

$\therefore$ There exists no +ve integer 'n' such that $na=0\ \forall a\in R$.

$\therefore$ Char. of $R=0$ $(\because Ka=a(K1))$

Case(ii) Let $O(1)=p\ (\neq 0)$ when the unit element 1 is regarded as an element of $(R,+)$.
By the defn of order of an element in a group. 'p' is the least +ve integer such that $p(1)=0$.
Now $m\in N$ (or I^+)
$m<p \Rightarrow m(1)\neq 0$

$$\begin{aligned}\forall a\in R,\ pa &= a+a+\cdots+a\ (p \text{ times})\\ &= a(1+1+\cdots+1)\\ &= a(p\cdot 1)\\ &= a(0)\\ &= 0\end{aligned}$$

Further $m\in N,\ m<p \Rightarrow ma\neq 0\ \forall a\in R$.
$\therefore$ ~~p is the least +ve integer~~ such that $pa=0\ \forall a\in R$.
$\therefore$ Char. of $R=p$.

Theorem → The Characteristic of an integral domain is either a prime or zero.

proof: Let $(R,+,\cdot)$ be an I.D.

If Char. of $R=0$ then there is nothing to prove.

Let Char $R = p$ $(p \neq 0)$. then 'p' is the least +ve integer such that $pa = 0 \;\; \forall a \in R$. ——— ①

Now we prove that 'p' is prime.

If possible suppose that p is not prime then $p = mn$; $1 < m, n < p$.

① ≡ $\forall a \in R$, $pa = 0$

$$\Rightarrow (mn)a = 0$$

$$\Rightarrow (mn)ab = 0b, \; b \in R$$

$$\Rightarrow ab + ab + \cdots + ab \; (mn \text{ times}) = 0 \quad \forall a, b \in R.$$

$$\Rightarrow \underbrace{(a+a+\cdots+a)}_{m \text{ times}}\underbrace{(b+b+\cdots+b)}_{n \text{ times}} = 0 \quad \forall a, b \in R$$

$$\Rightarrow (ma)(nb) = 0 \quad \forall a, b \in R. \text{ ——— ②}$$

for example $14ab = (2\cdot 7)ab$
$= ab + ab + ab + \cdots + ab$ $(2\times 7 \text{ times})$
$= \underbrace{(a+a)}_{2 \text{ times}}\underbrace{(b+b+\cdots+b)}_{7 \text{ times}}$

Since R is an I.D.

$\therefore R$ is without zero divisors

$\therefore$ ② ≡ either $ma = 0 \;\; \forall a \in R$ or $nb = 0 \;\; \forall b \in R$ where $1 < m < p$, $1 < n < p$.

$\therefore$ The above two statements contradict the fact that 'p' is the least +ve integer such that $pa = 0 \;\; \forall a \in R$.

$\therefore p$ must be a prime number.

Theorem → The Characteristic of a field is either zero or a prime number.

proof: Since every field is an I.D.

by the above theorem, the characteristic of a field is either zero or prime.

(Here we must provide the above theorem proof).

Theorem The characteristic of a division ring is either zero or prime.

proof: (The division ring has no zero divisors, with this help we can easily prove, The above theorem, total proof is applicable)

problems:

→ If R is a non-zero ring so that $a^2 = a \ \forall a \in R$ prove that characteristic of $R = 2$

Soln: Since $a^2 = a \ \forall a \in R$

we have $(a+a)^2 = a+a$

$\Rightarrow (a+a)(a+a) = a+a$

$\Rightarrow a(a+a) + a(a+a) = a+a$

$\Rightarrow (a^2+a^2) + (a^2+a^2) = a+a$

$\Rightarrow (a+a) + (a+a) = a+a. \quad (\because a^2 = a)$

$\Rightarrow (a+a) + (a+a) = (a+a) + 0$

$\Rightarrow a+a = 0 \quad (\because$ LCL in $(R,+,\cdot)$ i.e, $(R,+))$

$\Rightarrow 2a = 0$

$\therefore$ for every $a \in R$

we have $2a = 0$

Further $a \neq 0$, $1a = a \neq 0$

i.e, $1a \neq 0$

$\therefore$ 2 is the least +ve integer such that $2a = 0 \ \forall a \in R$.

$\therefore$ Char $R = 2$.

Note: The char. of a Boolean ring $= 2$.

→ If the characteristic of a ring R is '2' and the elements a, b of the ring commute. Prove that $(a+b)^2 = a^2+b^2 = (a-b)^2$.

Sol: Since the Char of R = 2

$\therefore 2x = 0 \ \forall x \in R$

$a, b \in R$ commute $\Rightarrow ab = ba$.

Now, we have

$(a+b)^2 = (a+b)(a+b)$
$= a(a+b) + b(a+b)$
$= (a^2+ab) + (ba+b^2)$
$= a^2+ab+ba+b^2$
$= a^2+ab+ab+b^2$ $(\because ab=ba)$
$= a^2+2ab+b^2$ —— (1)

Since for all $a, b \in R \Rightarrow ab \in R$
$\Rightarrow 2(ab) = 0$ $(\because 2x = 0 \ \forall x \in R)$

$\therefore$ (1) $\equiv$ $(a+b)^2 = a^2+0+b^2$
$= a^2+b^2$

Similarly we can prove that $(a-b)^2 = a^2+b^2$

→ If F is a field of characteristic p, p is a prime, then $(a+b)^p = a^p + b^p$ $\forall a, b \in F$.

Sol^n: Since F is a field,
Char. $F = p$; p is a prime.
$\therefore px = 0 \ \forall x \in F$ —— (1) where p is the least +ve integer

Now we have

$(a+b)^p = a^p + pa^{p-1}b + \frac{1}{2!}p(p-1)a^{p-2}b^2 + \cdots + pab^{p-1} + b^p$
$= a^p + (pb)a^{p-1} + \frac{1}{2!}(p-1)a^{p-2}b(pb) + \cdots + (pa)b^{p-1} + b^p$
$= a^p + b^p$ (by (1))

2000 → Prove that order of a finite field F is p^n, for some prime 'p' and some +ve integer 'n'.

Sol^n: Given that F is a field (finite)
Now we prove that Char $F \neq 0$
If possible, let Char $F = 0$
$\therefore$ By def^n ∄ +ve integer 'n' such that
$na = 0$ $\forall a \neq 0 \in F$
i.e, $na \neq 0$ $\forall a \in F$ & $\forall n \in N$ —— (1)

It follows that $a, 2a, 3a, \ldots$ belong to F.

Since F is finite

we must have $ia = ja$ for some +ve integers $i \& j$; $i > j$

$\Rightarrow (i-j)a = 0$

$\Rightarrow a = 0 \quad (\because i-j > 0)$

which is contradiction.

$\therefore$ Char $F \neq 0$.

W.K.T the characteristic of a field F is either zero or prime.

Since Char $F \neq 0$

$\therefore$ Char $F = p$ where p is prime number.

Here p is the smallest +ve integer such that $pa = 0 \; \forall a \in F$.

$\Longrightarrow O(a) = p$; Treating $(F, +)$ as a group

Since $(F, +)$ is a finite group.

$\therefore$ By Lagrange's theorem $O(a)$ divides $O(F)$.

i.e., p divides $O(F)$; where p is prime.

$\therefore O(F) = p^n$ for some $n \in N$.

Note: If R is finite (non-zero) integral domain then $O(R) = p^n$ where p is prime number and n is +ve integer.

$\longrightarrow$ If F is a finite field, its characteristic must be a prime number 'p' and F contains p^n elements for some integer 'n'. Further P.T. if $a \in F$ then $a^{p^n} = a$.

Sol^n: W.K.T $O(F) = p^n$

Since the non-zero elements of F (which are $p^n - 1$ in number)

form a $\times^{ve}$ group.

$\therefore$ By Lagrange's theorem

$a \in F \Rightarrow a^{p^n - 1} = e$ (multiplicative identity of F)

Hence $a \cdot a^{p^n - 1} = ae$

$\Rightarrow a^{p^n} = a$; $a \in F$

Set - VIII

IDEALS

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S of a ring R is called a left ideal of R, if

(i) $(S,+)$ is a subgroup of $(R,+)$

i.e. $\forall\, a,b \in S \Rightarrow a-b \in S$

(ii) $s \in S$ and $r \in R \Rightarrow rs \in S$.

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S' of a ring R is called a right ideal of R if

(i) $(S,+)$ is a subgroup of $(R,+)$

i.e. $\forall\, a,b \in S \Rightarrow a-b \in S$

(ii) $s \in S$ and $r \in R \Rightarrow sr \in S$

* **Definition:** Let $(R,+,\cdot)$ be a ring. A non-empty subset S of a ring R is called an ideal (or) a two sided ideal of R, if

(i) $(S,+)$ is a subgroup of $(R,+)$

i.e. $\forall\, a,b \in S \Rightarrow a-b \in S$

(ii) $s \in S$ and $r \in R \Rightarrow sr \in S$ and $rs \in S$.

In otherwords, a non-empty subset S of a ring R is an ideal of R, if S is both a left and right ideal of R.

→ R is a ring

(i) if $S = R \subseteq R$,

(i) $(R,+)$ itself is a subgroup of $(R,+)$

(2) $s \in R, r \in R \Rightarrow r.s \in R$ & $s.r \in R$

$\therefore$ R itself is an ideal of R

→ If R is a ring then R itself is an ideal of R. R is called unit ideal of R

(ii) If $S = \{0\} \subseteq R$,

(1) $0, 0 \in S \Rightarrow 0 - 0 = 0 \in S$

(2) $0 \in S, r \in R \Rightarrow 0r = 0 \in S$ & $r0 = 0 \in S$.

$\therefore S = \{0\}$ is an ideal of R.

→ $S = \{0\}$ is called null ideal of R (or) zero ideal of R

Note: (1) If R is a ring then the null ideal $\{0\}$ and the unit ideal R are called improper ideals of R.

Any other ideal of R is called a proper ideal of R.

(2) Every ring R always possesses two ideals (improper ideals)

(3) If R is a commutative ring, every ~~left~~ ideal is also a right ideal. Therefore in a commutative ring every left ideal or right ideal is a two-sided ideal.

Examples:

→ If I be the ring of integers and n be any fixed integer, then $S = (n) = \{nx \mid x \in I\}$ is an ideal of I.

Sol^n: Given that I is a ring

and $S = \{nx \mid x \in I\} \subseteq I$ where n is fixed integer.

Now let $a, b \in S$ choosing $a = nx$

$b = ny$; $x, y \in I$ & n is a fixed integer.

then $a - b = nx - ny$

$= n(x-y)$

$\in S$ ($\because x, y \in I \Rightarrow x - y \in I$)

$\therefore S$ is a subgroup of I.

Now let $r \in I$, $a \in S$, choosing $a = nx$; $x \in I$ & n is fixed integer.

then $ra = r(nx) = (rn)x$

$= (nr)x$

$= n(rx)$

$\in S \quad (\because rx \in I)$

and $ar = (nx)r = n(rx)$

$\in S \quad (\because rx \in I)$

$\therefore \forall\ a \in S$ and $r \in I$

$\Rightarrow ra \in S$ and

$ar \in S$

$\therefore S$ is an ideal of R and this ideal is a proper ideal.

Note: $(2) = \{ \ldots -6, -4, -2, 0, 2, 4 \ldots \}$,

$(3) = \{ \ldots -9, -6, -3, 0, 3, 6, 9 \ldots \}$ etc are Ideals in I.

→ The set of integers I is only a subring but not an ideal of the ring of rational numbers $(Q, +, \cdot)$

Sol'n: The product of a rational number and an integer is not necessarily an integer.

For example: $3 \in I$, $\frac{2}{5} \in Q$

$\Rightarrow \left(\frac{2}{5}\right)3 = \frac{6}{5} \notin I$

$\therefore I$ is not an Ideal of the ring of rational numbers.

Note: (1) The set Q of rational numbers is only a subring but not an ideal of the ring of real numbers $(R, +, \cdot)$

(2) The set IR of real numbers is only a subring but not an ideal of the ring of complex numbers $(C, +, \cdot)$.

Theorem: Every ideal of a ring R is a subring of R, but the converse need not be true.

Proof: Let S be an ideal of the given ring R.

Let $a, b \in S$, by definition of ideal $a-b \in S$.

further $a \in S$ and $b \in S \subseteq R$ (i.e. $b \in R$)

$$\Rightarrow ab \in S.$$

$\therefore S$ is a subring of R.

But the converse is not true,

i.e. Every subring need not be an ideal.

For example:

The set I of integers is a subring of the ring Q of rational numbers.

But I is not an ideal of Q.

Since $3 \in I$, $\frac{1}{2} \in Q \Rightarrow 3 \cdot \frac{1}{2} = \frac{3}{2} \notin I$.

Theorem: If S is an ideal of a ring R with unit element and $1 \in S$ then $S = R$.

Proof: Given that R is a ring with unity and S is ideal of R

$$\therefore S \subseteq R \quad \text{--- (1)}.$$

Let $r = x \in R$, $s = 1 \in S$ (by hyp)

$$\Rightarrow rs = x \cdot 1$$
$$= x \in S$$

and $s \cdot r = 1 \cdot x$

$$= x \in S \quad (\because S \text{ is an ideal})$$

$\therefore x \in R \Rightarrow x \in S$

$\therefore R \subseteq S$ --- (2)

$\therefore$ From (1) & (2), we have

$$R = S$$

Theorem: A field has no proper ideals

(or)

The ideals of a field F are only $\{0\}$ and F itself.

Proof: Let F be a field.

Let S be an ideal of F, so that $S=\{0\}$.

Now we prove that $S=F$:

By definition of ideal $S \subseteq F$ —— ①

Let $S \neq \{0\}$

$\therefore S$ contains non-zero element

Let $a(\neq 0) \in S \subseteq F \Rightarrow a(\neq 0) \in F$

$\Rightarrow a^{-1} \in F$ ($\because$ the non-zero elts of F have inverse w.r.t x^n in F)

Let $r = a^{-1} \in F$, $s = a \in S$

$\Rightarrow rs = a^{-1}a$

$= 1 \in S$

and $sr = aa^{-1}$

$= 1 \in S$ ($\because S$ is an ideal of F)

$\therefore \boxed{1 \in S}$

Now let $r = x \in F$, $s = 1 \in S$

$\Rightarrow rs = x \cdot 1$

$= x \in S$

and $s \cdot r = x \cdot 1$

$= x \in S$ ($\because S$ is an ideal of F)

$\therefore x \in F \Rightarrow x \in S$

$\therefore F \subseteq S$ —— ②

$\therefore$ From ① and ②, we have

Head Off.: A-31-34, 306, Top Floor, Jaina Extension, Dr. Mukherjee Nagar, Delhi-9.
Branch Off.: 87, First Floor (Back Side), Old Rajender Nagar Market, Delhi-110060
09999329111, 09999197625

$\therefore S = F$

$\therefore$ A field F has no proper ideals.

Theorem The intersection of two left ideals of a ring R is left ideal of R.

Proof: Let R be the given ring.

Let S_1 and S_2 be two left ideals of a ring R.

Let $S = S_1 \cap S_2$

Let $a, b \in S \Rightarrow a, b \in S_1 \cap S_2$

$\Rightarrow a, b \in S_1$ and $a, b \in S_2$

$\Rightarrow a - b \in S_1$ and $a - b \in S_2$

$\Rightarrow a - b \in S_1 \cap S_2$

$\therefore S$ is a subgroup of R.

(ii) $r \in R, s \in S \Rightarrow r \in R, s \in S_1 \cap S_2$

$\Rightarrow r \in R, (s \in S_1$ and $s \in S_2)$

$\Rightarrow (r \in R, s \in S_1)$ and $(r \in R, s \in S_2)$

$\Rightarrow r.s \in S_1$ and $rs \in S_2$ ($\because S_1$ & S_2 are an left ideals of R)

$\Rightarrow r.s \in S_1 \cap S_2$

$\Rightarrow rs \in S$

$\therefore S$ is a left ideal of R.

Note: (1) The intersection of two right ideals of a ring R is a right ideal of R

(2) The intersection of two ideals of a ring R is also an ideal of R

Theorem: The intersection of an arbitrary family of left ideals of a ring R is a left ideal of R.

Proof: Let S_1, S_2, S_3 ------ be left ideal of a ring R.

Let $S = S_1 \cap S_2 \cap S_3 \cap$ ------

$= \bigcap_{i \in N} S_i$

Let $a, b \in S \Rightarrow a, b \in \bigcap_{i\in N} S_i$

$\Rightarrow a, b \in S_i \;\forall\, i \in N$

$\Rightarrow a-b \in S_i \;\forall\, i\in N$ ($\because S_i$ is a subgroup)

$\Rightarrow a-b \in S$

$\therefore S$ is a subgroup of R.

Let $r \in R, s \in S$

$\Rightarrow r \in R,\; s \in \bigcap_{i\in N} S_i$

$\Rightarrow r \in R,\; s \in S_i \;\forall\, i \in N$

$\Rightarrow rs \in S_i \;\forall\, i \in N$ ($\because S_i$ is a left ideal)

$\Rightarrow rs \in \bigcap_{i\in N} S_i$

$\Rightarrow rs \in S$

$\therefore S = \bigcap_{i\in N} S_i$ is a left ideal.

<u>Note</u>: (1) The intersection of an arbitrary family of right ideals of a ring R is a right ideal of R.

(2) The intersection of an arbitrary family of ideals of a ring R is an ideal of R.

Imp Note: union of two ideals of a ring R need not be an ideal of R.

we know that

$A = (2) = \{ ---- -4, -2, 0, 2, 4, ---\} = \{2n / n \in I\}$

$B = (3) = \{ ---- -9, -6, -3, 0, 3, 6, 9, ---\} = \{3n / n \in I\}$

are two ideals of a ring I of integers.

Now $A \cup B = \{ - - - 9, -6, -4, -3, -2, 0, 3, 4, 6, 9, - - - \}$

Now $2, 3 \in A \cup B$

$\Rightarrow 3 - 2 = 1 \notin A \cup B$

$\therefore A \cup B$ is not ideal of I.

2013 → The union of two ideals of a ring R is an ideal of R if and only if one is contained in the other.

Proof: Let S_1 and S_2 be two ideals of the ring R.

— Let $S_1 \subset S_2$ or $S_2 \subset S_1$

if $S_1 \subset S_2$ then $S_1 \cup S_2 = S_2$ (S_2 is an ideal of R).

if $S_2 \subset S_1$ then $S_1 \cup S_2 = S_1$ (S_1 is an ideal of R)

$\therefore S_1 \cup S_2$ is an ideal of R.

Conversely suppose that $S_1 \cup S_2$ is an ideal of R.

Now we prove that $S_1 \subset S_2$ or $S_2 \subset S_1$

If possible, suppose that $S_1 \not\subset S_2$ or $S_2 \not\subset S_1$

since $S_1 \not\subset S_2$

Let $a \in S_1$ but $a \notin S_2$

since $S_2 \not\subset S_1$.

Let $b \in S_2$ but $b \notin S_1$

Now $a \in S_1$ and $b \in S_2 \Rightarrow a, b \in S_1 \cup S_2$

$\Rightarrow a - b \in S_1 \cup S_2$ ($\because S_1 \cup S_2$ is an ideal of R)

$\Rightarrow a - b \in S_1$ or $a - b \in S_2$

Now $a \in S_1$ and $a - b \in S_1$

$\Rightarrow a - (a - b) = b \in S_1$ ($\because S_1$ is an ideal of R)

$\therefore$ which is contradiction to the fact $b \notin S_1$.

Now $b \in S_2$; $a - b \in S_2$

$\Rightarrow b + (a - b) \in S_2$ ($\because S_2$ is an ideal of R)

$\Rightarrow a \in S_2$.

which is contradiction to fact $a \notin S_2$.

$\therefore$ our Supposition is wrong.

Hence $S_1 \subset S_2$ or $S_2 \subset S_1$.

Theorem: If R is commutative ring and $a \in R$ then $R = \{ra / r \in R\}$ is an ideal of R.

Proof: Given that R is commutative ring, $a \in R$

Now we Prove that $Ra = \{ra / r \in R\}$ is an ideal of R

For $0 \in R$, $0a \in Ra$

$\Rightarrow 0 \in Ra$

$\therefore Ra \neq \phi$ and $Ra \subseteq R$

Let $x, y \in Ra$ choosing $x = r_1 a$

$y = r_2 a$; $r_1, r_2 \in R$

then $x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a$

$\in Ra$ ($\because r_1, r_2 \in R \Rightarrow r_1 - r_2 \in R$)

$\therefore Ra$ is a subgroup of R w.r.t $+^n$.

Now let $x \in R$, $y \in Ra$ choosing $y = ra$, $r \in R$;

then $xy = x(ra)$

$= (xr)a$

$= (rx)a$ ($\because R$ is commutative ring i.e. $x \in R, r \in R \Rightarrow xr = rx$)

$\in Ra$ ($\because rx \in R$)

Similarly $yx \in Ra$

$\therefore Ra$ is an ideal of R.

Note: (1) If R is a commutative ring and $a \in R$ then $aR = \{ar / r \in R\}$ is an ideal of R.

(2) If R is a ring and $a \in R$ then Ra is a left ideal and aR is a right ideal.

1979

Theorem: A commutative ring R with unit element is a field if R has no proper ideals.

Proof: Given that R is a commutative ring with unity and R has no proper ideals.

Now we prove that R is a field.

For this we are enough to prove that the non-zero elements of R possesses inverse w.r.t '$\times$'.

Let $a (\neq 0) \in R$,

Let $Ra = \{ra / r \in R\} \subseteq R$

Let $x, y \in Ra$; choosing $x = r_1 a$

$y = r_2 a$; $r_1, r_2 \in R$

then $x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a \in Ra$ $\quad (\because r_1 - r_2 \in R)$

$\therefore Ra$ is a subgroup of R w.r.t. '$+$'.

Let $x \in R$, $y \in Ra$ choosing $y = ra$; $r \in R$

then $xy = x(ra)$

$= (xr)a$

$= (rx)a \quad (\because R$ is commutative ring$)$

$\in Ra \quad (\because x \in R, a \in R \Rightarrow xa \in R)$

Similarly $yx \in Ra$

$\therefore Ra$ is an ideal of R.

Since $(a\neq 0)\in R$, $1\in R$

$\Rightarrow 1.a \in Ra$

$\Rightarrow a\in Ra$

$\therefore$ Ra contains non-zero elements of R.

$\therefore Ra \neq \{0\}$

Since R has no proper ideals.

$\therefore Ra = R$.

Let the one of the element of R be I ($\because$ R is ring with unity)

Let $ba = 1$ for some $b\in R$.

Since R is commutative

$\therefore ba = ab = 1$

$\Rightarrow a^{-1} = b$

$\therefore$ the non-zero elements of R have inverses w.r.t $\times^n$.

$\therefore$ R is a field.

Note: If R is a ring with unit element and R has no proper ideals then R is a division ring.

Theorem. The sum of two ideals of a ring R is an ideal of R

(or)

If S_1 and S_2 are two ideals of a ring R, then $S_1+S_2 = \{x+y \mid x\in S_1, y\in S_2\}$ is an ideal of R.

Proof: Given that S_1 and S_2 are two ideals of a ring R

$S_1+S_2 = \{x+y \mid x\in S_1, y\in S_2\}$

Since $0\in R$ be the zero element

then $0 \in S_1$, $0 \in S_2 \Rightarrow 0+0 \in S_1+S_2$

$\Rightarrow 0 \in S_1+S_2$

$\therefore S_1+S_2 \neq \phi$ and subset of R.

Let $a, b \in S_1+S_2$ choosing $a = x_1+y_1$

$b = x_2+y_2$; $x_1, x_2 \in S_1$, $y_1, y_2 \in S_2$

then $a-b = (x_1+y_1)-(x_2+y_2)$

$= (x_1-x_2)+(y_1-y_2)$

$\in S_1+S_2$ $(\because x_1-x_2 \in S_1 \; ; \; y_1-y_2 \in S_2)$

$\therefore S_1+S_2$ is a subgroup of R.

Let $a \in R$, $b \in S_1+S_2$ choosing $b = x+y$; $x \in S_1$ & $y \in S_2$

then $ab = a(x+y)$

$= ax+ay$ $(\because ax \in S_1, ay \in S_2)$

$\in S_1+S_2$

similarly $ba \in S_1+S_2$

$\therefore S_1+S_2$ is an ideal of R

Note: since $S_1 \subseteq S_1+S_2$ and $S_2 \subseteq S_1+S_2$

$\therefore S_1+S_2$ is an ideal of R containing both S_1 and S_2

P.P.G → If S is an ideal of ring R and T any subring of R, then prove that S is an ideal of $S+T = \{s+t \,/\, s \in S, t \in T\}$

1814 Theorem If S_1 and S_2 are two ideals of ring R, then their product $S_1 S_2$ defined as

$S_1 S_2 = \{a_1 b_1 + a_2 b_2 + \dots + a_n b_n \,/\, a_i \in S_1, b_i \in S_2$ and $1 \leq i \leq n$ & n is positive integer$\}$

is an ideal of R.

Proof: Since S_1 & S_2 are two ideals of R.

$\therefore 0 \in S_1$ and $0 \in S_2$

$\Rightarrow 0 = 0 \cdot 0 \in S_1 \cdot S_2$

$\Rightarrow 0 \in S_1 \cdot S_2$

$\therefore S_1 S_2 \neq \phi$ and subset of R.

Let $x, y \in S_1 S_2$ choosing $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

$y = \alpha_1 \beta_1 + \alpha_2 \beta_2 + \cdots + \alpha_m \beta_m$

where $a_i \in S_1$, $b_i \in S_2$

$\alpha_j \in S_1$, $\beta_j \in S_2$

$1 \le i \le n$, $1 \le j \le m$ } n, m are +ve integer.

then $x - y = (a_1 b_1 + a_2 b_2 + \cdots + a_n b_n) - (\alpha_1 \beta_1 + \alpha_2 \beta_2 + \cdots + \alpha_m \beta_m)$

$= a_1 b_1 + a_2 b_2 + \cdots + a_n b_n + (-\alpha_1)\beta_1 + (-\alpha_2)\beta_2 + \cdots + (-\alpha_m)\beta_m$

$= x_1 y_1 + x_2 y_2 + \cdots + x_k y_k$ ($\because k = m + n$)

($\because x_l \in S_1$, $y_l \in S_2$, $1 \le l \le k$, l is +ve integer.

$\therefore x - y \in S_1 S_2$

$\therefore S_1 \cdot S_2$ is a subgroup of R.

Let $r \in R$, $x \in S_1 S_2$ choosing $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

$a_i \in S_1$, $b_i \in S_2$

$1 \le i \le n$;

n is +ve integer

then $rx = r(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)$

$= (ra_1)b_1 + (ra_2)b_2 + \cdots + (ra_n)b_n$

$= c_1 b_1 + c_2 b_2 + \cdots + c_n b_n$

where $c_1 = ra_1$, $c_2 = ra_2, \ldots, c_n = ra_n$ and c is belong to S_1, $1 \le i \le n$.

$\in S_1 S_2$

Similarly $xr \in S_1 S_2$

$\therefore S_1 S_2$ is an ideal of R.

→ If A and B are two ideals of a ring R, then $AB \subseteq A \cap B$

Proof: Given that R is a ring and A & B are ideals of R.

$\therefore AB$ and $A \cap B$ are ideals of R.

Now we prove that $AB \subseteq A \cap B$

Let $x \in AB$ then $x = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$

where $a_i \in A$, $b_i \in B$; $1 \le i \le n$, n is +ve integer.

Now $a_i \in A$, $b_i \in R \Rightarrow a_i b_i \in A$ ($\because A$ is right ideal of R)

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in A$

$\Rightarrow x \in A$

Now $a_i \in R$, $b_i \in B \Rightarrow a_i b_i \in B$ ($\because B$ is left ideal of R)

$\Rightarrow a_1 b_1 + a_2 b_2 + \cdots + a_n b_n \in B$

$\Rightarrow x \in B$

$\therefore x \in A \cap B$

$\because x \in AB \Rightarrow x \in A \cap B$

$\therefore AB \subseteq A \cap B$

→ If A and B are two ideals of a ring R, then $AB \subseteq A+B$

Sol'n: Given that R is a ring and A & B are ideals of R.

$\therefore$ AB and A+B are also ideals of R.

Now we prove that $AB \subseteq A+B$

let $x \in AB$ then $x = a_1b_1 + a_2b_2 + \dots + a_nb_n$ where $a_i \in A, b_i \in B$, $1 \le i \le n$.

Now $a_1 \in A, b_1 \in R \Rightarrow a_1b_1 \in A$ ($\because$ A is right ideal of R)

Again $a_i \in R, b_i \in B \Rightarrow a_ib_i \in B$; $2 \le i \le n$ ($\because$ B is right ideal of R)

$\Rightarrow a_2b_2 + a_3b_3 + \dots + a_nb_n \in B$

$\therefore a_1b_1 + (a_2b_2 + a_3b_3 + \dots + a_nb_n) \in A+B$

$\Rightarrow x \in A+B$

$\therefore$ if $x \in AB$ then $x \in A+B$

Hence $AB \subseteq A+B$

2007 → Let $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in Z \right\}$. Show that R is a ring under matrix addition and multiplication.

Let $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\}$. Then show that A is a left ideal of R but not a right ideal of R.

Sol'n: Let $R = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} / a, b, c, d \in Z \right\}$

Now we show that R is a ring w.r.t $+^n$ and $\times^n$.

(i) Closure Prop:

$\forall A, B \in R \Rightarrow A+B \in R$

$\therefore$ R is closed under $+^n$

(ii) Associative Prop: $\forall A, B, C \in R \Rightarrow (A+B)+C = A+(B+C)$

$\therefore$ R is associative under $+^n$.

(iii) Existence of left Identity :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$; $a, b, c, d \in Z$

$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in R$, $0 \in Z$ then

$$O + A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$= \begin{bmatrix} 0+a & 0+b \\ 0+c & 0+d \end{bmatrix}$$

$$= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (\because 0, a \in Z \Rightarrow 0+a = a)$$

$$= A$$

$\therefore \forall A \in R$, $\exists O$ (null matrix) $\in R$ such that

$O + A = A$.

$\therefore$ Identity prop. is satisfied w.r.t. +n.

Here O (null matrix) is the left identity in R.

(iv) Existence of left Inverse :

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$, $a, b, c, d \in Z$

$B = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} \in R$, $-a, -b, -c, -d \in Z$ then

$$B + A = \begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix} + \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} -a+a & -b+b \\ -c+c & -d+d \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \quad (\because -a+a = -b+b = -c+c + -d+d = 0)$$

$$= O$$

$\therefore \forall A \in R$, $\exists B = -A \in R$ such that

$B + A = O$.

$\therefore B = -A$ is left inverse of A in R w.r.t +n.

(V) Commutative Prop:

$$\forall A, B \in R \Rightarrow A+B = B+A$$

$\therefore (R, +)$ is an abelian group.

(II) (i) closure Prop:

$$\forall A, B \in R \Rightarrow A \cdot B \in R$$

(ii) Associative Prop:

$$\forall A, B, C \in R \Rightarrow (A \cdot B) \cdot C = A \cdot (B \cdot C)$$

$\therefore (R, \cdot)$ is a semigroup.

(III) Distributive laws:

$$\forall A, B, C \in R$$

$$\Rightarrow A \cdot (B+C) = A \cdot B + A \cdot C$$

R satisfies DL

$\therefore (R, +, \cdot)$ is a ring.

Given that $A = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} / a, b \in Z \right\} \subseteq R$

Since $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in A$

$\therefore A \neq \phi$.

Now $A_1, A_2 \in A$ choosing $A_1 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}$, $A_2 = \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$ $a_1, b_1, a_2, b_2, 0 \in Z$

then $A_1 - A_2 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} - \begin{bmatrix} a_2 & 0 \\ b_2 & 0 \end{bmatrix}$

$$= \begin{bmatrix} a_1 - a_2 & 0 \\ b_1 - b_2 & 0 \end{bmatrix} \in A \quad (\because a_1 - a_2, b_1 - b_2 \in Z)$$

IMS (INSTITUTE OF MATHEMATICAL SCIENCES)
Head Off.: A-31-34, 306, Top Floor, Jaina Extension, Dr. Mukherjee Nagar, Delhi-9.
Branch Off.: 87, First Floor (Back Side), Old Rajender Nagar Market, Delhi-110060
09999329111, 09999197625

$\therefore$ A is a subgroup of R.

Let $A_1 = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} \in A$, $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in R$

$a_1, b_1 \in Z$ $\qquad\qquad a, b, c, d \in Z$

then $BA_1 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix} = \begin{bmatrix} aa_1+bb_1 & 0 \\ ca_1+db_1 & 0 \end{bmatrix}$

$\in A \; (\because aa_1+bb_1, ca_1+db_1 \in Z)$.

$\therefore$ A is the left ideal in R.

Now $A_1B = \begin{bmatrix} a_1 & 0 \\ b_1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$= \begin{bmatrix} a_1a & a_1b \\ b_1a & b_1b \end{bmatrix} \notin A$

$\therefore$ A is not the right ideal in R.

H.W → Show that the set $S = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in I \right\}$ is a right ideal of M_2, the ring of 2×2 matrices over integers, which is not a left ideal of M_2.

→ Let R be a ring and $a \in R$, show that the set $S = \{ r \in R \;/ ra = 0 \}$ is a left ideal of R.

Sol'n: Since $0a = 0$

$\therefore 0 \in S$

$\Rightarrow S \neq \phi$ and subset of R.

Now let $r_1, r_2 \in S$; $r_1a = 0$; $r_2a = 0$.

Now $(r_1 - r_2)a = r_1a - r_2a$

$= 0 - 0$

$= 0$

$\therefore \boxed{r_1 - r_2 \in S}$

$\therefore$ S is a subgroup of R.

For any $r \in R$ and $x \in S$,

$$(rx)a = r(xa)$$
$$= r(0)$$
$$= 0$$

$\therefore \boxed{rx \in S}$

Hence S is a left ideal of R.

→ Let R be the ring of all real valued, continuous functions on $[0,1]$. Show that the set $S = \{f \in R / f(\frac{1}{2}) = 0\}$ is an Ideal of R.

Sol^n: Let $f, g \in S$. Then $f(\frac{1}{2}) = 0$ and $g(\frac{1}{2}) = 0$ —— ①

consider $(f-g)(\frac{1}{2}) = f(\frac{1}{2}) - g(\frac{1}{2})$

$$= 0 - 0$$
$$= 0 \quad (\text{by } ①)$$

$\therefore (f-g)(\frac{1}{2}) = 0$

$\Rightarrow \boxed{f-g \in S}$

$\therefore$ S is a subgroup of R.

Let $f \in S$ and $h \in R$. Then

$$(fh)(\tfrac{1}{2}) = f(\tfrac{1}{2})\, h(\tfrac{1}{2})$$
$$= 0 \cdot h(\tfrac{1}{2}) \quad (\text{by } ①)$$
$$= 0$$

$\therefore (fh)(\frac{1}{2}) = 0$

$\Rightarrow \boxed{fh \in S}$

Now $(hf)(\frac{1}{2}) = h(\frac{1}{2}) f(\frac{1}{2})$

$$= h(\tfrac{1}{2}) \cdot 0 \quad (\text{by } ①)$$
$$= 0$$

$\therefore \boxed{hf \in S}$

$\therefore fh, hf \in S \ \forall f \in S$ and $h \in R$

Hence S is an ideal of R.

→ Let R be the ring of all real valued continuous functions on $[0,1]$. Show that the set $S = \{f \in R \mid f(2/3) = 0\}$ is an ideal of R

→ If U is an ideal of R, then prove that $r(U) = \{x \in R \mid xu = 0 \ \forall u \in U\}$ is an ideal of R.

Sol'n: Since $0u = 0 \ \forall u \in U$

$\therefore 0 \in r(U)$

$\therefore r(U) \neq \phi$ and subset of R

Let $x, y \in r(U)$; $xu = 0$, $yu = 0 \ \forall u \in U$ —— ①

Now we have

$$(x-y)(u) = x(u) - y(u)$$
$$= 0 - 0 \ \forall u \in U \ (\text{by } ①)$$
$$= 0$$

$\therefore (x-y)(u) = 0$

$\therefore \boxed{x - y \in r(U)}$

$r(U)$ is a subgroup of R.

Let $a \in R$ and $x \in r(U)$, so that $xu = 0 \ \forall u \in U$ —— ②

Now $(ax)u = a(xu)$

$= a(0)$ (by ②)

$= 0$

$\therefore (ax)u = 0 \ \forall u \in U$

$\Rightarrow ax \in r(U)$

Again $(xa)u = x(au)$

$= xy$ where $y = au$.

Since U is an ideal of R,

So $a \in R$ and $u \in U \Rightarrow au \in U$

$\Rightarrow y \in U$ —— ③

from ② and ③, we have,

$xy = 0$

$\Rightarrow x(au) = 0$

$\Rightarrow (xa)u = 0$

$\therefore (xa)u = 0 \ \forall \ u \in U$

$\Rightarrow xa \in r(U)$

Hence $r(U)$ is an ideal of R.

HW → If R is a ring and L is a left ideal of R. then $\lambda(L) = \{x \in R \,/\, xa = 0 \ \forall \ a \in L\}$ is a two-sided ideal.

→ If U is an ideal of R, then Prove that $[R:U] = \{x \in R \,/\, rx \in U \text{ for every } r \in R\}$ is an ideal of R and that it contains U.

Sol'n: Since U is an ideal of R,

so $0 \in U$, i.e. $r0 \in U \ \forall \ r \in R$

$\therefore 0 \in [R:U]$

and $[R:U] \neq \phi$ and subset of R.

Let $x, y \in [R:U]$, $rx \in U, ry \in U \ \forall \ r \in R$ ——— ①

Since U is an ideal of R.

$\therefore rx - ry \in U \ \forall \ r \in R$.

Now $r(x-y) = rx - ry \in U \ \forall \ r \in R$.

$\Rightarrow x - y \in [R:U]$

$\therefore [R:U]$ is a subgroup of R.

Using (1), $(ra)x \in U$ $(\because ra \in R)$

we have

$r(ax) = (ra)x \in U \ \forall \ r \in R$

$\Rightarrow \boxed{ax \in [R:U]}$

Since U is an ideal of R,

So $rx \in U$ and $a \in R$

$\Rightarrow (rx)a \in U \Rightarrow r(xa) \in U \quad \forall r \in R$

$\Rightarrow \boxed{xa \in [R:U]}$

Hence $[R:U]$ is an ideal of R.

Now we show that $U \subseteq [R:U]$

Let $x \in U$. Then $rx \in U \ \forall r \in R$ ($\because U$ is an ideal of R)

Now $rx \in U \ \forall r \in R$

$\Rightarrow x \in [R:U]$

$\Rightarrow U \subseteq [R:U]$

Hence $[R:U]$ is an ideal of R containing U.

→ Prove that $Z(R)$, the centre of a ring R, is only a subring of R and need not be an Ideal of R.

Sol^n: By definition, $Z(R) = \{a \in R \,/\, xa = ax \ \forall x \in R\}$

It can be easily shown that $Z(R)$ is a subring of R. (Workdone by student)

Let M_2 be the ring of all 2×2 matrices over the integers.

For any $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2$ and

$A = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} \in M_2$.

Now $Ax = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ap & bp \\ cp & dp \end{pmatrix}$

$= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix} = xA$

Hence $Z(M_2) = \left\{ \begin{bmatrix} p & 0 \\ 0 & p \end{bmatrix} \,/\, p \text{ is integer} \right\}$

Now we show that $Z(M_2)$ is not an ideal of M_2.

For $S = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in M_2$, $A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \in Z(M_2)$

we have

$$SA = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix} \notin Z(M_2)$$

Hence $Z(M_2)$ is not an ideal of M_2.

→ Let A and B be two ideals of a commutative ring R with unity such that $A+B=R$.

show that $AB = A\cap B$.

Sol^n: Given that A and B are two ideals of a commutative ring R with unity such that $A+B=R$.

Now we show that $AB = A\cap B$

Since A and B are two ideals of R

$\therefore AB \subseteq A\cap B$ —— ①

Let $x \in A\cap B$ be arbitrary

Since $R = A+B$ and $1 \in R$

$\therefore 1 \in A+B$

$\Rightarrow 1 = a+b$ for some $a\in A$ & $b \in B$

Now $x = x.1$

$= x(a+b)$

$= xa + xb$ —— ①

since $x\in A$ and $b\in B \Rightarrow xb \in AB$

$x\in B$ and $a \in A \Rightarrow ax \in AB$

$\Rightarrow xa \in AB$ ($\because$ R is commutative)

$\therefore xa + xb \in AB$ ($\because$ AB is an ideal of R)

$\therefore$ By ①, $x\in AB$

$\therefore x \in A\cap B \Rightarrow x \in AB$

$\therefore A\cap B \subseteq AB$ —— (2)

$\therefore$ from (1) & (2) we have

$$AB = A\cap B$$

Note: Two ideals A and B of a ring R satisfying $A+B=R$ are called co-maximal ideal.

* If A, B and C are ideals of a ring R, Prove that $A(B+C) = AB+AC$.

Sol'n: Since A, B and C are ideals of a ring R.

$\therefore$ $B+C$, AB, AC, $A(B+C)$ and $AB+AC$ are also ideals of R.

For any $b\in B$, $b = b+0 \in B+C$ $\quad(\because 0\in C)$

$\therefore B\subseteq B+C$ —— (1)

Similarly $C\subseteq B+C$ —— (2)

from (1) & (2) we have

$AB\subseteq A(B+C)$

and $AC\subseteq A(B+C)$

$\Rightarrow AB+AC \subseteq A(B+C)$ —— (3)

Now let $x\in A(B+C)$ be arbitrary.

Then $x = a_1t_1 + a_2t_2 + \cdots + a_nt_n$ where $a_i\in A$, $t_i\in B+C$.

Since $t_i\in B+C$

$\therefore t_i = b_i + c_i$ for some $b_i\in B$, $c_i\in C$

$\therefore x = a_1(b_1+c_1) + a_2(b_2+c_2) + \cdots + a_n(b_n+c_n)$

$= (a_1b_1 + a_2b_2 + \cdots + a_nb_n) + (a_1c_1 + a_2c_2 + \cdots + a_nc_n)$

$\in AB+AC$

$\therefore A(B+C) \subseteq AB+AC$ —— (4)

$\therefore$ from (3) & (4) we have

$$A(B+C) = AB+AC.$$

→ 7. If A, B, C are ideals of a ring R such that $B \subseteq A$, Prove that $A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$.

Sol'n: Given that A, B, C are ideals of a ring R. Such that $B \subseteq A$

$\therefore B+C$, $A \cap C$ and $A \cap (B+C)$, $B + (A \cap C)$ are ideals of R.

Let $x \in A \cap (B+C)$

Then $x \in A$ and $x \in B+C$

we have $x \in B+C \Rightarrow x = b+c$, for some $b \in B$, $c \in C$.

Thus $b+c \in A$ $(\because x \in A)$

and $b \in A$ $(\because B \subseteq A)$

$\Rightarrow b+c-b \in A$ ($\because A$ is an ideal of R)

$\Rightarrow c \in A$

$\therefore$ we have $c \in C$ & $c \in A$

$\Rightarrow c \in A \cap C$

$\because x = b+c \Rightarrow x \in B + (A \cap C)$;

$\therefore A \cap (B+C) \subseteq B + (A \cap C)$ —— ①

Let $x \in B + (A \cap C)$

$\Rightarrow x = b_1 + c_1$, for some $b_1 \in B$, $c_1 \in A \cap C \Rightarrow c_1 \in A$ & $c_1 \in C$

$\Rightarrow x \in B+C$ as $b_1 \in B$, and $c_1 \in C$

Again $B \subseteq A \Rightarrow b_1 \in A$, Also $c_1 \in A$

$\Rightarrow x = b_1 + c_1 \in A$, as A is an ideal of R.

Thus $x \in A$ and also $x \in B+C$

$\Rightarrow x \in A \cap (B+C)$

$\therefore B + (A \cap C) \subseteq A \cap (B+C)$ —— ②

from ① & ②

We obtain $A \cap (B+C) = B + (A \cap C)$

Since $B \subseteq A$, so $A \cap B = B$.

Hence $A \cap (B+C) = B + (A \cap C) = (A \cap B) + (A \cap C)$

→ Let R be a commutative ring and let A be an ideal of R. Show that

$\sqrt{A} = \{x \in R \mid x^n \in A$ for some positive integer $n\}$ is an ideal of R such that (i) $A \subseteq \sqrt{A}$ (ii) $\sqrt{\sqrt{A}} = \sqrt{A}$ (iii) If R has unity and $\sqrt{A} = R$, then $A = R$

Sol'n: Let $a, b \in \sqrt{A}$

Then $a^m \in A$ and $b^n \in A$, for some positive integers m and n.
Since R is commutative ring.

$$(a-b)^{m+n} = a^{m+n} - (m+n)C_1 a^{m+n-1} b + \cdots + (-1)^{m+n} b^{m+n}$$

$$= a^m . a^n - (m+n) C_1 a^m a^{n-1} b + \cdots + (-1)^{m+n} b^m b^n \in A$$

($\because a^m \in A, b^n \in A$ and A is an ideal of R)

$\therefore a - b \in \sqrt{A}$

For any $r \in A$, $a \in \sqrt{A}$,
we have $(ra)^m = r^m a^m$, since R is commutative.
Again $r^m a^m \in A$, ($\because a^m \in A$, $r^m \in R$ and A is an ideal of R)
$\therefore ra \in \sqrt{A}$
Similarly $ar \in \sqrt{A}$
Hence $\sqrt{A}$ is an ideal of R.

(i) Obviously, $A \subseteq \sqrt{A}$ ($\because x \in A \Rightarrow x^n \in A$, as A is an ideal of R)

(ii) we have $\sqrt{\sqrt{A}} = \sqrt{S}$ where $S = \sqrt{A}$.

By part (i) $S \subseteq \sqrt{S} \Rightarrow \sqrt{A} \subseteq \sqrt{\sqrt{A}}$, —— ①

let $x \in \sqrt{\sqrt{A}} \Rightarrow x \in \sqrt{S} \Rightarrow x^n \in S$, for some $n \in N$.

$\Rightarrow x^n \in \sqrt{A}$

$\Rightarrow (x^n)^m \in A$, for some $m \in N$

$\Rightarrow (x^{nm}) \in A$, where $nm \in N$

$\Rightarrow x \in \sqrt{A}$

$\therefore$ we have $x \in \sqrt{\sqrt{A}} \Rightarrow x \in \sqrt{A}$

$\Rightarrow \sqrt{\sqrt{A}} \subseteq \sqrt{A}$ —— ②

$\therefore$ from (1) & (2)

$$\sqrt{\sqrt{A}} = \sqrt{A}$$

(iii) Let $1 \in R$ and $\sqrt{A} = R$

Then $1 \in \sqrt{A} \Rightarrow 1^n \in A$, for some positive integer n.

$\Rightarrow 1 \in A$ and A is an ideal of R

$\Rightarrow 1.r \in A \;\; \forall r \in R$

$\Rightarrow r \in A \;\; \forall r \in R$

$\Rightarrow R \subseteq A$

Obviously

Hence $A = R$

Note: $\sqrt{A}$ is often called the radical of A.

→ Let R be a ring with unity. If R has no right ideals except R and $\{0\}$,

then prove that R is a division ring.

(or)

Let R be ring with unit element, R not necessarily commutative, such that the only right ideals of R are $\{0\}$ and R. Prove that R is a division ring.

Sol'n: Given that R is a ring with unit element and R has no right ideals except R and $\{0\}$.

i.e. R has ideals $\{0\}$ and R.

Now we prove that R is a division ring

For this we are enough to prove that the non-zero elements of R possesses inverse w.r.t $\times^n$.

Let $a (\neq 0) \in R$

Let $aR = \{ar \mid r \in R\} \subseteq R$ ——— (1)

Since $0 \in R$, $a(0) \in aR$

$\Rightarrow 0 \in aR$

$\therefore aR \neq \phi$

$\therefore aR$ is a non-empty subset of R.

Let $x, y \in aR$: choosing $x = ar_1$

$y = ar_2$; $r_1, r_2 \in R$

then we have $x - y = ar_1 - ar_2$

$= a(r_1 - r_2)$

$\in aR$ $(\because r_1 - r_2 \in R)$

$\therefore (aR, +)$ is a subgroup of $(R, +)$

Let $x \in R$, $y \in aR$ choosing $y = ar$; $r \in R$

then $yx = (ar)x$

$= a(rx)$

$\in aR$ $(\because r \in R, x \in R \Rightarrow rx \in R)$

$\therefore aR$ is a right ideal of R

Since $a(\neq 0) \in R$; $1 \in R$

$\therefore a \cdot 1 \in aR$

$\Rightarrow a \in aR$

$\therefore aR$ contains non-zero elements of R.

$\therefore aR \neq \{0\}$

Since R has no proper right ideals.

$\therefore aR = R$.

Let one of the element of aR be 1. ($\because R$ is ring with unity)

Let $ab = 1$ for some $b \in R$ ——— ①

From ①, it follows that each non-zero element of R has a right inverse.

Since $b(\neq 0) \in R$ (for otherwise, $1 = ab = 0$, a contradiction)

there exists some $c \in R$ such that $bc = 1$ ——— ②

Now we have

$ba = ba \cdot 1$; 1 is the unity of R.

$= (ba)(bc)$ (by ②)

$= b(ab)c$ (by associative of R)

$= b(1)c$ (by ①)

$= bc$

$= 1$ (by ②)

$\therefore ab = ba = 1$

$\Rightarrow a^{-1} = b \in R$

Hence R is a division ring.

Note: Let R be a ring with unity. If R has no left ideals except R and {0}, then prove that R is a division ring.

→ Let R be a ring having more than one element such that $aR = R \;\forall\; a \neq 0 \in R$, then R is a division ring.

Sol^n: Firstly we shall show that

$x \neq 0$ and $y \neq 0$ in R

$\Rightarrow x.y \neq 0$

(or)

$xy = 0 \Rightarrow$ either $x = 0$ or $y = 0$, $x, y \in R$ ——— ①

If $x \neq 0$ and $y \neq 0$ then by given hypothesis

$xR = R$, $yR = R$ ——— ②

Now we have

$0 = xy \Rightarrow 0 \cdot R = (xy)R$

$= x(yR)$

$= xR$ (by ②)

$= R$ (by ②)

$\therefore 0 \cdot R = R$.

$\therefore R=\{0\}$, a contradiction to the fact that R has more than one element.

Hence ① is Proved.

Since $R \neq \{0\}$

i.e. R contains non-zero elements.

$\exists$ some $a \neq 0 \in R$ such that $aR=R$

Now $a\in R \Rightarrow a \in aR$

$\Rightarrow a = ae$ for some $e \in R$

It may be noted that

$e \neq 0$, for otherwise $a = a0 = 0$, a contradiction.

$\therefore ae = a$

$\Rightarrow ae^2 = ae$

$\Rightarrow a(e^2-e)=0$

$\Rightarrow e^2-e=0$ (by ①)

$\Rightarrow e^2=e$ ——— ②

Let $x \in R$ be arbitrary. then

$(xe-x)e = xe^2 - xe$

$= xe - xe$

$= 0$ (by ②)

$\therefore (xe-x)e = 0$

Since $e \neq 0$ and using ①,

$xe - x = 0$

$\Rightarrow xe = x \;\forall\; x \in R$

$\Rightarrow e$ is the right identity of R. ——— ③

Now we shall show that each non-zero element of R has a right inverse.

Let $x \neq 0 \in R$ then by given hypothesis,

$xR = R$

Since $e \in R$, $e \in xR$

$\Rightarrow e = xy$ for some $y \in R$

$\Rightarrow y$ is the right inverse of x. ——— ④

from ③ and ④, it follows that

R is a division ring.

* **Ideal Generated By a Subset of Ring:**

Let S be a subset of a ring R. An ideal U of the ring R is said to be generated by 'S' if (i) $S \subseteq U$

(ii) for any ideal V of R, $S \subseteq V$ $\Rightarrow U \subseteq V$

The ideal U generated by S is, denoted by (S) or $<S>$ or $\{S\}$ or $(S) = U$

Indeed, $<S>$ is the smallest ideal containing 'S'.

→ If A and B are any two ideals of a ring R. show that A+B is an ideal of R generated by $A \cup B$. i.e. $A+B = (A \cup B)$

Sol'n: Given that A and B are two ideals of the ring R.

∴ A+B is also an ideal of R.

For any $a \in A$ $\Rightarrow a = a + 0 \in A+B$

$\therefore A \subseteq A+B$ —— ①

Similarly $B \subseteq A+B$ —— ②

from ① & ② we have

$A \cup B \subseteq A+B$ —— ③

Let I be any ideal of R such that $A \cup B \subseteq I$ —— ④

Now we shall prove that $A+B \subseteq I$ —— ⑤

Let $x \in A+B$ then $x = a+b$, $a \in A$, $b \in B$.

Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$

$\therefore a, b \in A \cup B$

$\Rightarrow a, b \in I$ from (4)

from ③ and ④, it follows that

R is a division ring.

* Ideal Generated By a Subset of Ring:

Let S be a subset of a ring R. An ideal U of the ring R is said to be generated by 'S' if (i) $S \subseteq U$

(ii) for any ideal V of R, $S \subseteq V$
$\Rightarrow U \subseteq V$

The ideal U generated by S is denoted by (S) or $\langle S \rangle$ or $\{S\}$ or $(S) = U$

Indeed, $\langle S \rangle$ is the smallest ideal containing 'S'.

→ If A and B are any two ideals of a ring R. show that $A+B$ is an ideal of R generated by $A \cup B$. i.e. $A+B = (A \cup B)$.

Sol'n: Given that A and B are two ideals of the ring R.

$\therefore$ $A+B$ is also an ideal of R.

For any $a \in A$, $a = a + 0 \in A+B$

$\therefore A \subseteq A+B$ —— ①

Similarly $B \subseteq A+B$ —— ②

from ① & ② we have

$A \cup B \subseteq A+B$ —— ③

Let I be any ideal of R such that $A \cup B \subseteq I$ —— ④

Now we shall prove that $A+B \subseteq I$ —— ⑤

Let $x \in A+B$ then $x = a+b$, $a \in A$, $b \in B$.

Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$

$\therefore a, b \in A \cup B$

$\Rightarrow a, b \in I$ from (4)

Theorem: If R is commutative ring with unit element and $a \in R$, then the set $U = \{ra / r \in R\}$ is a principal ideal of R generated by the element 'a'.

Proof: For $1 \in R$, $1a = a \in U$

Let $x, y \in U$ and $s \in R$

Then $x = r_1 a$, $y = r_2 a$; where $r_1, r_2 \in R$

Now $x - y = r_1 a - r_2 a$

$= (r_1 - r_2) a$

$= r' a \in U$ where $r' = r_1 - r_2 \in R$

Now $sx = s(r_1 a)$

$= (sr_1) a$

$= r'' a \in U$, where $r'' = sr_1 \in R$

Since R is commutative,

$sx = xs$

$\therefore U$ is ideal of R

Let V be any other ideal of R such that $a \in V$

Now we shall show that $U \subseteq V$

Now $x \in U \Rightarrow x = r_1 a \in U$ where $r_1 \in R$

Since $a \in V$, $r_1 \in R$

and V is an ideal.

$\therefore r_1 a \in V$

$\Rightarrow x \in V$

$\therefore x \in U \Rightarrow x \in V$

$\Rightarrow U \subseteq V$.

Hence U is principal ideal of R generated by 'a'

Note: (1). If R is Commutative ring with unity and $a \in R$ then the set $\{ar / r \in R\}$ is the principal ideal generated by 'a' as $\{ar / r \in R\} = \{ra / r \in R\}$.

(2) If R is Commutative ring and $a \in R$ then the $\{ra + na / r \in R, n \in R\}$ is the principal ideal of R generated by 'a'.

Example: $R = I$ is a commutative ring of integers with unit element. i.e. $R = \{ \cdots -3, -2, -1, 0, 1, 2, 3 \cdots \}$

$S_1 = \{2n / n \in I\} = \{ \cdots -6, -4, -2, 0, 2, 4, 6, \cdots \}$

$S_2 = \{3n / n \in I\} = \{ \cdots -9, -6, -3, 0, 3, 6, 9 \cdots \}$

$S_3 = \{4n / n \in I\} = \{ \cdots -12, -8, -4, 0, 4, 8, 12 \cdots \}$

$S_4 = \{6n / n \in I\} = \{ \cdots -18, -12, -6, 0, 6, 12, 18 \cdots \}$

Now

(1) $6 \in S_4 \subseteq S_2$, $S_4 \subseteq S_1$, $S_4 \subseteq I$

$\therefore S_4 = (6)$.

(2) $3 \in S_2 \subseteq I$

$\therefore S_2 = (3)$

(3) $4 \in S_3 \subseteq S_1 \subseteq I$

$\therefore S_3 = (4)$

(4) $S_1 = (2)$ $\quad (\because S_1 \subseteq I)$

* Principal Ideal Ring:

A ring R is called a principal ideal ring if every ideal in R is a principal ideal.

A ring R is called a principal ideal ring if every ideal in R is a Principal ideal.

* Principal Ideal Domain (PID):

A commutative ring without zero divisors and with unity element is a principal ideal domain, if every ideal S in R is a principal ideal

i.e. if every ideal S in R is of the form $S = (a)$ for some $a \in S$.

Theorem: Every field is a principal ideal domain.

Proof: We know that a field has no proper ideals.

i.e. the ideals of the field F are $\{0\}$ and F.

Let S be an ideal of R.

- If $S = \{0\}$ then it is a principal ideal generated by '0'.
- If $S \neq \{0\}$ then S contains non-zero elements.

Let $a(\neq 0) \in S \subseteq F$ —— ①

$\therefore a^{-1}$ exists in F

$\therefore a^{-1} \in F,\ a(\neq 0) \in S \Rightarrow a^{-1}a \in S$ $(\because S$ is an ideal$)$

$\Rightarrow 1 \in S$

$\therefore F \subseteq S$ —— ②

$\therefore$ from ① & ② we have

$F = S$

$\therefore$ the other ideal containing 1 is F

i.e. $S = F = (1)$

$\therefore$ The two ideals of F are principal ideals.

$\therefore F$ is a PID.

* for example: $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are principal ideal domains.

Theorem: The ring of integers is a PID.

(or)

Every ideal of the ring of integers is a principal ideal.

Given that I be the ring of integers.

and I is commutative ring with unity and without zero divisors.

Let S be an ideal of I.

If $S=\{0\}$ then it is a principal ideal generated by '0'.

If $S\neq\{0\}$ then S contains non-zero elements.

Let $a(\neq 0)\in S$

$\Rightarrow -a\in S$ ($\because$ the ideal S is additive subgroup of I)

$\therefore$ S contains +ve and −ve integers.

Let s be the least +ve integer in S.

Let P be any element in 'S'

$\therefore$ By division algorithm, $\exists$ integers q, r

such that $P = sq + r$ $(0\leq r < s)$

Now $q\in I$, $s\in S \Rightarrow sq\in S$ & $qs\in S$ ($\because S$ is an ideal)

$P\in S$, $sq\in S \Rightarrow P - sq\in S$ ($\because S$ is subgroup of $(I,+)$)

$\Rightarrow r\in S$ where $0\leq r<s$

which contradicts the fact s is the least +ve integer that belongs to S.

$\therefore r=0$

$\therefore P = sq$

$\therefore P\in S \Rightarrow P = sq$ for some $q\in I$.

Hence S is a principal ideal of I generated by s.

i.e. $S = (s)$

Quotient Rings (or) Rings of Residue Classes:

Suppose R is an arbitrary ring and 'S' is an ideal (two sided ideal) in R. Then S is a subgroup of the additive abelian group of R.

therefore if $a \in R$ then the set

$S+a = \{s+a \mid s \in S\}$ is called right coset of S in R.

Since R is abelian group w.r.t $+^n$

$$S+a = a+S$$

i.e. the right coset is same as left coset.

We call $S+a$ as simply a coset of S in R.

Note: (1) if $a, b \in R$ then $S+a = S+b \Leftrightarrow a-b \in S$

(2) $a \in S \Leftrightarrow S+a = S$.

The cosets of S in R are called the residue classes of S in R.
The set of all residue classes of S in R is denoted by the symbol $\frac{R}{S}$.

i.e. $\frac{R}{S} = \{S+a \mid a \in R,\ S \text{ is an ideal of } R\}$

Theorem: If S is an ideal of a ring R, then the set $\frac{R}{S} = \{S+a \mid a \in R\}$ of all residue classes of S in R forms a ring for the two compositions in $\frac{R}{S}$ defined as follows:

$(S+a)+(S+b) = S+(a+b)$ —① (addition of residue classes)

$(S+a)(S+b) = S+ab$ —② (multiplication of residue classes)

Proof: First of all, we shall show that both $+^n$ and $\times^n$ in $\frac{R}{S}$ are well defined.

For this we are to show that

if $S+a = S+a'$ and

$S+b = S+b'$ then

$(S+a)+(S+b) = (S+a')+(S+b')$

and $(S+a)(S+b) = (S+a')(S+b')$

Now we have

$S+a = S+a' \Rightarrow a' \in S+a$ $\quad [\because a' = 0+a' \in S+a'$
$\Rightarrow a' \in S+a' = S+a$
$\Rightarrow a' \in S+a]$

and $S+b = S+b' \Rightarrow b' \in S+b$

$\therefore \exists\ \alpha, \beta \in S$ such that $a' = \alpha + a$, $b' = \beta + b$

Now $a'+b' = (\alpha+a) + (\beta+b)$

$= (a+b) + (\alpha+\beta)$

$\Rightarrow (a'+b') - (a+b) = (\alpha+\beta) \in S \quad (\because \alpha, \beta \in S)$

$\Rightarrow (a'+b') - (a+b) \in S$

$\Rightarrow \boxed{S+(a'+b') = S+(a+b)}$

$\Rightarrow (S+a') + (S+b') = (S+a) + (S+b)$

$\therefore$ addition in $\frac{R}{S}$ is well defined.

Again $a'b' = (\alpha+a)\cdot(\beta+b)$

$= \alpha\beta + \alpha b + a\beta + ab$

$= ab + \alpha\beta + \alpha b + a\beta$

$\Rightarrow a'b' - ab = \alpha\beta + \alpha b + a\beta \in S$ ($\because S$ is an ideal therefore $\alpha, \beta \in S$ and $a, b \in R \Rightarrow \alpha b \in S, a\beta \in S, \alpha\beta \in S$ $\Rightarrow \alpha\beta + \alpha b + a\beta \in S$)

Since $a'b' - ab \in S$

$\Rightarrow S + a'b' = S + ab$

$\Rightarrow (S+a')(S+b') = (S+a)(S+b)$

Hence multiplication in $\frac{R}{S}$ is well defined.

(i) Let $S+a, S+b \in \frac{R}{S}$; $a, b \in R$

then $(S+a) + (S+b) = S + (a+b)$ (by ①)

$\in \frac{R}{S} \quad (\because a+b \in R)$

and $(S+a)(S+b) = S+(ab)$ (by ②)

$\in \frac{R}{S} \quad (\because ab \in R)$

$\therefore$ closure is satisfied w.r.t $+^n$ & $\times^n$.

(ii) Let $s+a, s+b, s+c \in \frac{R}{S}$; $a,b,c \in R$

then $(s+a)+[(s+b)+(s+c)] = (s+a)+[s+(b+c)]$

$= s+[a+(b+c)]$

$= s+[(a+b)+c]$ ($\because$ R is a ring)

$= [s+(a+b)]+(s+c)$

$= [(s+a)+(s+b)]+(s+c)$

Associative property is satisfied w.r.t $+^n$.

(iii) $0 \in R \Rightarrow s+0 = s \in \frac{R}{S}$

Now $(s+a)+(s+0) = s+(a+0)$

$= s+a$ ($\because a+0=a \ \forall a \in R$)

Similarly $(s+0)+(s+a) = s+a$.

$\therefore \forall (s+a) \in \frac{R}{S}, a \in R$, $\exists$ $s+0 = s \in \frac{R}{S}$, $0 \in R$

such that $(s+a)+(s+0) = s+a = (s+0)+(s+a)$

Identity property is satisfied w.r.t $+^n$.

Here $s+0 = s$ is the identity element in $\frac{R}{S}$.

(iv) $a \in R \Rightarrow -a \in R$

$\forall s+a \in \frac{R}{S}$, $\exists$ $s+(-a) \in \frac{R}{S}$ such that

$(s+a)+[s+(-a)] = s+[a+(-a)]$

$= s+0$ ($\because a+(-a)=0$ in R)

Similarly $[s+(-a)]+(s+a) = s+0$

$\therefore$ Inverse property is satisfied in $\frac{R}{S}$ w.r.t $+^n$

Here $s+(-a)$ is the inverse of $s+a$ in $\frac{R}{S}$.

(v) Let $s+a, s+b \in \frac{R}{S}$, $a, b \in R$ then

$$(s+a)+(s+b) = s+(a+b)$$
$$= s+(b+a) \quad (\because R \text{ is a ring})$$
$$= (s+b)+(s+a)$$

$\therefore$ Commutative property is satisfied w.r.t $+^n$.

$\therefore \left(\frac{R}{S}, +\right)$ is an abelian group.

(ii) Let $s+a, s+b, s+c \in \frac{R}{S}$, $a, b, c \in R$

then $(s+a)[(s+b)(s+c)] = (s+a)[s+(bc)]$ (by ②)

$$= s+[a(bc)] \quad \text{by ②}$$
$$= s+[(ab)c]$$
$$= (s+(a.b))(s+c)$$
$$= [(s+a)(s+b)](s+c)$$

$\therefore$ Associative property is satisfied in $\frac{R}{S}$ w.r.t $\times^n$.

$\therefore \left(\frac{R}{S}, \times\right)$ is a semigroup.

(iii) Let $s+a, s+b, s+c \in \frac{R}{S}$, $a, b, c \in R$

then $(s+a)[(s+b)+(s+c)] = (s+a)\cdot[s+(b+c)]$

$$= s+[a.(b+c)]$$
$$= s+[a.b+a.c] \quad (\because R \text{ is a ring})$$
$$= (s+(ab))+(s+(ac))$$
$$= [(s+a).(s+b)]+[(s+a).(s+c)]$$

Similarly $[(s+b)+(s+c)]\cdot(s+a) = (s+b)\cdot(s+a)+(s+c)\cdot(s+a)$

$\therefore$ Multiplication is distributive w.r.t $+^n$ in $\frac{R}{S}$.

$\therefore \left(\frac{R}{S}, +, \cdot\right)$ is a ring.

Definition: Let R be a ring and S be an ideal of R then the set $\frac{R}{S} = \{S+a \mid a\in R\}$ of all residue classes of S in R is a ring for the two compositions in R defined as follows

$(S+a)+(S+b) = S+(a+b)$ (addition of residue classes)

$(S+a)\cdot(S+b) = S+(ab)$ (multiplication of residue classes)

This ring $(\frac{R}{S};+,\cdot)$ is called the quotient ring or factor ring or residue class ring.

Note: It is convenient, sometimes, to denote coset (residue class) $S+a$ in $\frac{R}{S}$ by the symbol $\bar{a}$ or $[a]$. Then we write sum and product of two cosets (residue classes) as $[a]+[b]=[a+b]$ and $[a].[b]=[ab]$

→ If $\frac{R}{S}$ is the quotient ring, Prove that:

(i) $\frac{R}{S}$ is commutative if R is commutative and

(ii) $\frac{R}{S}$ has unity element if R has unity element

(iii) $\frac{R}{S}$ is boolean ring if R is the quotient ring

Sol'n: (i) Given that $\frac{R}{S}$ is the quotient ring and R is commutative.

Now we have

$\forall\ S+a,\ S+b\in\frac{R}{S};\ a,b\in R$

$\Rightarrow (S+a)(S+b) = S+(ab)$

$= S+(ba)$ ($\because R$ is commutative)

$= (S+b)\cdot(S+a)$

$\therefore \frac{R}{S}$ is commutative ring

(ii) Given that R has unity

i.e. $\forall\ a\in R,\ \exists\ 1\in R$ such that $a.1=1.a=a$

Now we have

$\forall\ s+a \in \frac{R}{S}$, $a\in R$, $\exists\ s+1 \in \frac{R}{S}$, $1\in R$.

such that $(s+a)(s+1) = s+(a1)$

$= s+a$ ($\because a1 = 1a = a$ in R)

Similarly $(s+1)(s+a) = s+a$.

$\therefore \frac{R}{S}$ has unity.

$\therefore s+1$ is the unity element in $\frac{R}{S}$.

(iii) we have $(s+a)^2 = (s+a)(s+a)$

$= s+a^2$

$= s+a$ ($\because a^2 = a\ \forall a\in R$)

$\forall\ s+a \in \frac{R}{S}$

$\therefore \frac{R}{S}$ is boolean ring.

→ Consider $Z_6 = \{0,1,2,3,4,5\}$, the ring of integers modulo 6. then $S=\{0,3\}$ is an ideal of Z_6. Determine the quotient ring $\frac{Z_6}{S}$

Sol'n: Given that $Z_6 = \{0,1,2,3,4,5\}$, the ring of integers modulo 6.

$S = \{0,3\} \subseteq Z_6$

Since S is a ring of Z_6.

$\therefore (S, +_6)$ is a subgroup of $(Z_6, +_6, \times_6)$

Now let $s\in S$, $r\in Z_6 \Rightarrow sr\in S$ & $rs\in S$

i.e. let $s = 3\in S$, $r = 4\in Z_6$

$\Rightarrow s.r = 3\times_6 4 = 0\in S$

& $rs = 0\in S$ etc

$\therefore S$ is an ideal of Z_6.

Now the cosets of S in R are as under:

$S+0 = \{0+0, 3+0\} = \{0,3\}$

$S+1 = \{0+1, 3+1\} = \{1,4\}$

$S+2 = \{0+2, 3+2\} = \{2,5\}$

$S+3 = \{0+3, 3+3\} = \{3,0\} = S+0$

$S+4 = \{0+4, 3+4\} = \{4,1\} = S+1$

$S+5 = \{0+5, 3+5\} = \{5,2\} = S+2$

$\therefore \frac{Z_6}{S} = \{S+0, S+1, S+2\}$ is the quotient ring.

→ Show that the set $S = \{5x \mid x \in Z\}$ is an ideal of Z. Determine the quotient ring $\frac{Z}{S}$.

Sol'n: It is easy to verify that 'S' is an ideal of Z.

Now we have

$S = \{\ldots -15, -10, -5, 0, 5, 10, 15, \ldots\}$

$S+1 = \{\ldots -14, -9, -4, 1, 6, 11, 16, \ldots\}$

$S+2 = \{\ldots -13, -8, -3, 2, 7, 12, \ldots\}$

$S+3 = \{\ldots -12, -7, -2, 3, 8, 13, 18 \ldots\}$

$S+4 = \{\ldots -11, -6, -1, 4, 9, 14, 19, \ldots\}$

$S+5 = \{\ldots -10, -5, 0, 5, 10, 15, \ldots\}$

$= S+0$

$S+6 = S+1$, $S+7 = S+2$ etc.

$\therefore \frac{Z}{S} = \{S+0, S+1, S+2, S+3, S+4\}$

Prime Ideal and Maximal Ideal:

→ Let R be a ring. An ideal P of a ring R is called a prime ideal, if for any $a \in R$, $b \in R$; $ab \in P \Rightarrow$ either $a \in P$ or $b \in P$.

For example:

(1) The ideal $P = \{0\}$ in Z (ring of integers) is a prime ideal.

Because, let $a, b \in Z$ such that $a \cdot b \in \{0\}$

$\Rightarrow ab = 0$

$\Rightarrow$ either $a = 0$ or $b = 0$

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

(2) For any prime number P,

$(P) = \{Px / x \in Z\}$ is a prime ideal of Z.

because, let $a, b \in Z$ be such that $ab \in (P)$

$\Rightarrow ab = px$ for some $x \in Z$

$\Rightarrow \frac{ab}{p} = x$ for some $x \in Z$

$\Rightarrow \frac{a}{p}$ or $\frac{b}{p}$

$\Rightarrow a = py$ or $b = pz$ ($\because$ P is prime) for some $y, z \in Z$

$\Rightarrow a \in (P)$ or $b \in (P)$

In particular, the ideals,

$(2) = \{----4, -2, 0, 2, 4, ----\}$

$(3) = \{-----6, -3, 0, 3, 6, ---\}$

$(5) = \{-----10, -5, 0, 5, 10, ---\}$ etc are prime ideals of Z.

(3) The ideal $(4) = \{----12, -8, -4, 0, 4, 8, ----\}$ is not a prime ideal of Z.

Since $2 \cdot 6 = 12 \in (4)$ but $2 \notin (4)$ and $6 \notin (4)$.

Theorem Let R be a commutative ring. Prove that an ideal P of R is a prime ideal iff R/P is an integral domain.

Proof: Given that R is the commutative ring and P is an ideal of R.

Let $\frac{R}{P}$ be an Integral Domain

we now prove that P is a prime ideal of R.

i.e. $a, b \in R$ and $ab \in P \Rightarrow a \in P$ or $b \in P$.

Now for any $a, b \in R$ and $ab \in P$

$\Rightarrow P+ab = P$ $(\because a \in P \Leftrightarrow P+a = P)$

$\Rightarrow (P+a)\cdot(P+b) = P+0$

$\Rightarrow (P+a) = P+0$ (or)

$P+b = P+0$ ($\frac{R}{P}$ is an ID)

$\Rightarrow a \in P$ (or) $b \in P$ $(P+a = P \Rightarrow a \in P)$

$\therefore$ P is a Prime ideal of R.

Conversely suppose that

let P be a prime ideal of R

we now Prove that $\frac{R}{P}$ is an integral domain.

$P+a, P+b \in \frac{R}{P}$; $a, b \in R$

$\Rightarrow (P+a)(P+b) = P+0$

$\Rightarrow P+ab = P+0$ $(\because S+a = S+b \Rightarrow a-b \in S)$

$\Rightarrow ab-0 \in P$

$\Rightarrow a \in P$ or $b \in P$ ($\because$ P is a Prime ideal)

$\Rightarrow P+a = P+0$ or $P+b = P+0$

$\therefore \frac{R}{P}$ has no zero divisors.

and hence $\frac{R}{P}$ is an ID.

$\Rightarrow P+a = P+0$ (or) $P+b = P+0$

$\therefore \frac{R}{P}$ has no zero divisors.

and hence $\frac{R}{P}$ is an ID.

* Maximal Ideal :

Let R be a ring and M be an ideal such that $M \neq R$. M is said to be a maximal ideal of R, if for any other ideal U of R such that $M \subset U \subset R$ then either $M = U$ (or) $U = R$.

In otherwords, an ideal $M \neq R$ is a maximal ideal of R, if there does not exist any proper ideal b/w M and R.

Note: ① An ideal M of a ring R is called a maximal ideal if M is not included in any other ideal of R excep R itself.

For example:

Let $R = I$ (ring of integers)

$S_1 = \{2n \mid n \in I\} = \{\ldots -6, -4, -2, 0, 2, 4, 6 \ldots\}$

$S_2 = \{3n \mid n \in I\} = \{\ldots -9, -6, -3, 0, 3, 6, 9 \ldots\}$

$S_3 = \{4n \mid n \in I\} = \{\ldots -12, -8, -4, 0, 4, 8, 12, \ldots\}$

$S_4 = \{5n \mid n \in I\} = \{\ldots -15, -10, 0, 10, 15 \ldots\}$

$S_5 = \{6n \mid n \in I\} = \{\ldots -18, -12, -6, 0, 6, 12, 18 \ldots\}$

Since $S_5 \subset S_2 \subset I$, $S_5 \subset S_1 \subset I$

$S_4 \subset I$, $S_3 \subset S_1 \subset I$

$S_2 \subset I$, $S_1 \subset I$.

$\therefore S_1, S_2$ and S_4 are maximal.

S_3 and S_5 are not maximals.

Example (2):

- $\{0, 2\}$ is a maximal ideal of the ring $Z_4 = \{0, 1, 2, 3\}$ modulo 4.
- $\{0, 4\}$ and $\{0, 2, 4, 6\}$ are maximal ideals of the ring.

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ mod 8.

($\because$ $\exists$ no proper ideals b/w $\{0,3\}$ and $\mathbb{Z}_8$ and $\{0,2,4,6\}$ and $\mathbb{Z}_8$).

further, $\{0,4\}$ is an ideal of $\mathbb{Z}_8$.

($\because$ $\{0,4\} \subset \{0,2,4,6\} \subset \mathbb{Z}_8$).

problems:

→ Find the maximal ideals of $\mathbb{Z}_6$, the ring of integers modulo 6.

Sol'n: Given that $\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ is the ring of integers $\mathbb{Z}_6$.

The Proper ideals of $\mathbb{Z}_6$ are

$(3) = \{0,3\}$; $(2) = \{0,2,4\}$

Since there does not exist any proper ideal between (3) and $\mathbb{Z}_6$, (2) and $\mathbb{Z}_6$

$\therefore$ $(3), (2)$ are maximal ideals of $\mathbb{Z}_6$.

→ Find the maximal ideals of $\mathbb{Z}_{12}$, the ring of integers modulo 12

Sol'n: Given that $\mathbb{Z}_{12} = \{0,1,2 \ldots 11\}$ is the ring of integers modulo 12.

The Proper ideals of $\mathbb{Z}_{12}$ are.

$(2) = \{0,2,4,6,8,10\}$

$(3) = \{0,3,6,9\}$

$(4) = \{0,4,8\}$

$(6) = \{0,6\}$

Since there does not exist any proper ideal between (3) and $\mathbb{Z}_{12}$

$\therefore$ (3) is the maximal ideal of $\mathbb{Z}_{12}$.

Similarly (2) is also a maximal ideal of $\mathbb{Z}_{12}$.

However (4) and (6) are not maximal ideals of $\mathbb{Z}_{12}$ [$\because$ $(4) \subset (2) \subset \mathbb{Z}_{12}$ and $(6) \subset (3) \subset \mathbb{Z}_{12}$.]

→ Show that $\{0\}$ is the only maximal ideal of a field F.

Sol'n: we know that a field F has only two ideals F and $\{0\}$.

Since $F \neq \{0\}$

$\{0\}$ is the only maximal ideal of F.

→ Show that $(4) = \{\ldots -8, -4, 0, 4, 8 \ldots\}$ is the maximal ideal of the ring E of even integers.

Sol'n: Since $2 \notin (4)$, $(4) \neq E$.

Let U be any other ideal of E

Such that $(4) \subset U \subset E$, $(4) \neq U$.

Then $\exists$ some $x \in U$ such that $x \notin (4)$

$\Rightarrow x$ is an even integer not divisible by 4.

$\Rightarrow x = 4n+2$ for some integer 'n'

$\Rightarrow 2 = x - 4n$, where $x - 4n \in U$ ($\because$ U is an ideal i.e $x \in U$, $4n \in U \Rightarrow x - 4n \in U$)

$\Rightarrow 2 \in U$

$\Rightarrow (2) \subseteq U$

$\Rightarrow E = U$

Hence (4) is ~~the~~ a maximal ideal of E.

Imp → Show that $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$ iff n_0 is a prime number.

Sol'n: Let n_0 be a prime number

we prove that $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$.

Such that $M \subset U \subset \mathbb{Z}$

Since $n_0 \in M$, $n_0 \in U \Rightarrow n_0 = nx$, for some $x \in \mathbb{Z}$

$\Rightarrow n = 1$ or $n = n_0$ ($\because n_0$ is prime)

If $n = 1$, then $U = (1) = \mathbb{Z}$

If $n = n_0$, then $U = M$

Hence $M = (n_0)$ is a maximal ideal of $\mathbb{Z}$

Conversely, let $M = (n_0)$ be a maximal ideal of $\mathbb{Z}$

we prove that n_0 is a prime number.

If possible, suppose that n_0 is a composite number

Let $n_0 = ab$, $a \neq \pm 1$, $b \neq \pm 1$

Let $U = (a)$ (it is obvious)

Suppose x is an arbitrary element of M

Then $x = n_0 r$ for some $r \in \mathbb{Z}$.

$\Rightarrow x = (ab) r$

$\Rightarrow x = a(br)$

$\Rightarrow x \in U$

$\therefore M \subseteq U \subseteq \mathbb{Z}$

Since M is a maximal ideal of $\mathbb{Z}$,

$\therefore$ either $M = U$ or $U = \mathbb{Z}$.

If $U = \mathbb{Z}$, then $a = 1$ which is a contradiction to $a \neq 1$.

If $U = M$, then $a = n_0 l$ for some integer l.

($\because$ Each element of M is multiple of n_0 i.e, $M = (n_0)$)

$\therefore n_0 = ab$

$= (n_0 l) b$

$= n_0 (lb)$

Since $n_0 \neq 0$

$\therefore lb = 1$

$\Rightarrow b = 1$

which is a contradiction.

$\therefore$ our assumption that n_0 is composite number is wrong.

Hence n_0 must be a prime integer.

<u>Note</u>: (1) For the ring of integers $\mathbb{Z}$, any ideal generated by prime integer is a maximal ideal.

(2) A ring may have more than one maximal ideal.

For eg: the ring $\mathbb{Z}$ has $\langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle, \ldots$ as maximal Ideals.

1988, 2001 → If R is a commutative ring with unity, then an ideal M of R is maximal iff $\frac{R}{M}$ is a field.

<u>Proof:</u> Given that R is a commutative ring with unity and M is an ideal.

∴ The quotient ring $\frac{R}{M} = \{a+M \mid a \in R\}$ is a commutative ring and has unity.

Zero element of $\frac{R}{M}$ is $0+M = M$ where $0 \in R$ is zero element in R.

unit element of $\frac{R}{M}$ is $1+M$ where $1 \in R$ is the unity element in R.

Now suppose that M is a maximal ideal of R.

We prove that $\frac{R}{M}$ is a field.

To prove that $\frac{R}{M}$ is a field, we have to show that every non zero element of $\frac{R}{M}$ has multiplicative inverse.

Let $a+M \in \frac{R}{M}$ and $a+M$ be non-zero element

$\therefore a+M \neq M$

$\Rightarrow a \notin M$ $\left(\because a+M \neq M \Leftrightarrow a \notin M \text{ (or) } M+a \neq M \Leftrightarrow a \notin M\right)$

If $\langle a \rangle = \{ar \mid r \in R\}$ is a principal ideal of R

then $\langle a \rangle + M$ is also an ideal of R (Since the sum of two ideals is again an ideal of R).

Again $a = a \cdot 1 + 0 \in \langle a \rangle + M$ and $a \notin M$

& $M \subset \langle a \rangle + M \subseteq R$

Since M is a maximal ideal of R

$\therefore \langle a \rangle + M = R$

Since $1 \in R \Rightarrow 1 \in \langle a \rangle + M$

$\Rightarrow 1 = ar + m$ for some $r \in R, m \in M$

$$\Rightarrow 1+M = (ar+m)+M$$
$$= (ar+M)+(m+M)$$
$$= (ar+M)+M \quad (\because m\in M \Leftrightarrow m+M=M)$$
$$= ar+M \quad (\because \text{By additive identity prop of } R/M)$$
$$= (a+M)(r+M)$$

$\therefore (a+M)(r+M) = (r+M)(a+M) = 1 \quad (\because R/M \text{ is Comm})$

$\Rightarrow (a+M)^{-1} = r+M \in \frac{R}{M}$

Hence every non-zero element of $\frac{R}{M}$ is invertible

$\therefore \frac{R}{M}$ is field.

Conversly suppose that $\frac{R}{M}$ is a field.

We prove that M is maximal ideal of R

Let U be any ideal of R such that

$M \subset U \subseteq R$ and $M \neq U$

Now we shall show that $U = R$

Since $M \subset U$ and $M \neq U$, $\exists\, p \in U$ s.t $p \notin M$

i.e. $p+M \neq M \quad (\because p+M = M \Leftrightarrow p\in M)$

i.e $p+M$ is non-zero element of $\frac{R}{M}$

Since $\frac{R}{M}$ is a field

and $p+M$ is non-zero element of $\frac{R}{M}$

$\Rightarrow p+M$ has multiplicative inverse, say $q+M$

$\therefore (p+M)(q+M) = 1+M$

$\Rightarrow pq+M = 1+M$

$\Rightarrow 1-pq \in M \quad (\because a+M = b+M \Leftrightarrow (-a)+b \in M)$

Since U is an ideal of R

So $p \in U$ and $q \in R$

$\Rightarrow pq \in U$.

$pq \in U$ and $1-pq \in U$

$\Rightarrow pq + (1-pq) \in U$

$\Rightarrow 1 \in U$.

$\therefore 1 \in U$ and U is an ideal of R

$\therefore U = R$ ($\because \forall\, x \in R$ and $1 \in U$
$\Rightarrow x \cdot 1 \in U$
$\Rightarrow x \in U$
$\therefore R \subset U$ & $U \subset R$
$\Rightarrow U = R$)

Hence M is Maximal ideal of R.

1991 → For a commutative ring with unity, maximal ideal is a prime ideal.

Sol: Let R be a commutative ring with unity

Let U be a Maximal ideal of R

then $\frac{R}{U}$ is a field.

Since every field is an integral domain.

$\therefore \frac{R}{U}$ is an integral domain.

$\Rightarrow U$ is a prime ideal

($\because$ Let R be a Comm. ring then an ideal P of R is prime ideal $\Leftrightarrow \frac{R}{P}$ is an integral domain)

Thus every maximal ideal is prime ideal.

Note 1 :- The converse of the above need not be true. i.e. for a commutative ring with unity, a prime ideal need not be maximal ideal.

Let us consider the integral domain of integers Z.

Then, the null ideal $= \langle 0 \rangle$ is a prime ideal, But $\langle 0 \rangle$ ideal is not maximal ideal, because, there exists ideal $\langle 2 \rangle$ so that

$$\langle 0 \rangle \subset \langle 2 \rangle \subset Z \text{ and } \langle 2 \rangle \neq \langle 0 \rangle, \; \langle 2 \rangle \neq Z.$$

Note (2): for a commutative ring without unity a maximal ideal need not be a prime ideal.

Sol: Let $E = \{2n / n \in Z\}$

$=$ the ring of even integers without unity element.

Let $(4) = (2)^2 = \{4n / n \in Z\}$

$= \{\cdots\cdots -8, -4, 0, 4, 8, \cdots\cdots\}$ be an ideal of E.

Since $2 \notin (4)$, $(4) \neq E$

Let U be any other ideal of E s.t.

$(4) \subset U \subset E$, $(4) \neq U$

Then $\exists$ some $x \in U$ s.t. $x \notin (4)$

$\Rightarrow$ x is an even integer not divisible by 4

$\Rightarrow$ $x = 4n+2$ for some integer 'n'

$\Rightarrow$ $2 = x - 4n$ ——— ①

Since $x \in U$, $4n \in (4)$ and $(4) \subset U$

$x \in U$, $4n \in U$

$\Rightarrow x - 4n \in U$ ($\because U$ is an ideal)

$\Rightarrow 2 \in U$ (by ①)

$\Rightarrow (2) \subset U$ —— ②

we know that $U \subset E = (2)$

From ② & ③, we have

$U = E$

$\therefore$ The ideal (4) is the maximal ideal

Now for $2, 2 \in E$

and $2 \cdot 2 = 4 \in (4)$

We do not have $2 \in (4)$.

$\therefore (4)$ is not prime ideal.

→ In a Commutative ring R with unity, if M is a maximal ideal & $x \in R$ then, prove that there exists $\alpha \in R$ such that $x \notin M \Rightarrow 1 - x\alpha \in M$.

Sol: Given that R is a commutative Ring with unity.

& M is maximal ideal of R

Let the principal ideal generated by $x \in R$ be $\langle x \rangle$

Since M, $\langle x \rangle$ are ideals of R

$\Rightarrow \langle x \rangle + M$ is ideal of R

Since M is maximal ideal of R

$\therefore \langle x \rangle + M = R$

Since $1 \in R \Rightarrow 1 \in \langle x \rangle + M$

$\therefore \exists\, a \in M$ and $\alpha \in R$

such that $x\alpha + a = 1$

$\therefore \exists\, \alpha \in R$ s.t $1 - x\alpha = a \in M$

$\Rightarrow 1 - x\alpha \in M$

Homomorphisms and Embedding of Rings

→ Let $(R, +, \cdot)$ and $(R', \oplus, \otimes)$ be two rings. mapping $f: R \to R'$ is said to be a homomorphism, if

(i) $f(a+b) = f(a) \oplus f(b)$,

(ii) $f(a \cdot b) = f(a) \otimes f(b) \ \forall \ a, b \in R$

The above conditions imply that f preserves the compositions of the rings R and R'.

However, if we agree to use the same compositions '+' and '·' for both R and R' then

→ A mapping $f: R \to R'$ is called a homorphism, if (i) $f(a+b) = f(a) + f(b)$

(ii) $f(a \cdot b) = f(a) \cdot f(b) \ \forall \ a, b \in R$

Note: The operations +, · on the left handside of the properties (i), (ii) are of the ring R, while the operations +, · on R.H.S of the properties (i), (ii) are those of the ring R'

→ A ring R' is called a homomorphic image of a ring R if there exists a homomorphism 'f' of R onto R'.

i.e. f is a homorphism and for each $r' \in R'$ there exists some $r \in R$ such that $f(r) = r'$.

→ A mapping $f: R \to R'$ is called an isomorphism, if (i) f is a homomorphism

(ii) f is 1-1 i.e. $f(a) = f(b) \Rightarrow a = b$ for $a, b \in R$.

→ A ring R' called an isomorphic image of the ring R, if there exists a mapping $f: R \to R'$ such that

(i) f is a homomorphism

(ii) f is a one - one and

(iii) f is onto

Note:- If $f: R \to R'$ is an onto homomorphism then R' is the homomorphic image of R and we write $R \simeq R'$.

→ If $f: R \to R'$ is $1-1$ + onto homomorphism then R' is isomorphic image of R or R is isomorphic to R' and we write $R \cong R'$.

→ If $f: R \to R'$ is an onto homomorphism then $f(R) = R'$.

→ If U is an ideal of the ring R, then $\frac{R}{U} = \{ x+U / x \in R \}$ is also a ring w.r.t addition and multiplication of cosets. Then the mapping $f: R \to \frac{R}{U}$ defined by $f(x) = x+U$ for all $x \in R$ is called the natural homomorphism from R onto $\frac{R}{U}$.

* Examples of Homomorphisms:

→ If R is a ring then the mapping $f: R \to R$ defined as $f(x) = x \; \forall \; x \in R$ is a homomorphism.

Sol:- For any $x, y \in R$

$f(x+y) = x+y = f(x)+f(y)$

and $f(xy) = xy = f(x)f(y)$.

$\therefore f$ is a homomorphism.

→ If R is a ring, the mapping $f: R \to R'$ defined as $f(x) = 0' \ \forall x \in R$ is a homomorphism.

Sol:- For any $x, y \in R$

$\Rightarrow x+y \in R$
$xy \in R$

$\therefore f(x) = 0', f(y) = 0'$

By definition, $f(x+y) = 0'$
$= 0'+0'$
$= f(x)+f(y)$.

and $f(xy) = 0'$
$= 0' \cdot 0'$
$= f(x)f(y)$

$\therefore f$ is a homomorphism from R into R'.

This is called zero homomorphism.

→ If $Z[\sqrt{2}] = \{m+n\sqrt{2} \,/\, m, n \in I\}$, the mapping $f: Z[\sqrt{2}] \to Z[\sqrt{2}]$ defined as $f(m+n\sqrt{2}) = m-n\sqrt{2}$ is a homomorphism.

Sol: Let $x, y \in Z[\sqrt{2}]$ Choosing
$x = a+b\sqrt{2}$
$y = c+d\sqrt{2}$, $a, b, c, d \in Z[\sqrt{2}]$

Then $x+y = (a+c)+(b+d)\sqrt{2}$

$xy = (ac+2bd)+(ad+bc)\sqrt{2}$

We have

$$f(x+y) = (a+c)-(b+d)\sqrt{2}$$
$$= (a-b\sqrt{2})+(c-d\sqrt{2})$$
$$= f(x)+f(y)$$

and $f(xy) = (ac+2bd)-(ad+bc)\sqrt{2}$
$$= (a-b\sqrt{2})(c-d\sqrt{2})$$
$$= f(x).f(y)$$

Thus f is a homomorphism.

→ Let $R = Z$ and R' = set of all even integers.

Then $(R', +, *)$ is a ring.

where $a*b = \frac{ab}{2}$ $\forall\ a,b \in R'$. The mapping $f: R \to R'$ defined as $f(a) = 2a$ $\forall\ a \in R$ is a homomorphism.

Sol:- for any $a, b \in R$,

We have $f(a+b) = 2(a+b)$
$$= 2a+2b$$
$$= f(a)+f(b)$$

and $f(ab) = 2(ab)$
$$= \frac{(2a)(2b)}{2}$$
$$= (2a)*(2b)$$
$$= f(a)*f(b)$$

Thus f is a homomorphism.

Properties of Homomorphism:-

Theorem 1: Let $f: R \to R'$ be a homomorphism of a ring R into the ring R' and $0' \in R'$ be the zero elements Then

(1). $f(0) = 0'$

(2). $f(-a) = -f(a) \ \forall a \in R$

(3). $f(a-b) = f(a) - f(b) \ \forall a, b \in R$

Sol^n (1) Since $0 \in R$. We have

$$0+0 = 0$$
$$f(0+0) = f(0)$$
$$\Rightarrow f(0)+f(0) = f(0) + 0', \ f(0) \in R'$$
$$\Rightarrow f(0) = 0' \ (\text{by LCL of } R')$$

(2) Since $a \in R$, $-a \in R$ such that

$$a + (-a) = 0$$
$$f(a+(-a)) = f(0)$$
$$\Rightarrow f(a) + f(-a) = 0'$$
$$\Rightarrow \boxed{f(-a) = -f(a)}$$

(3) For $a, b \in R$, $f(a-b) = f(a) + f(-b)$
$$= f(a) - f(b).$$

Theorem 2: If f is a homomorphism from a ring R into R' then $f(R)$ is a subring of R'.

Sol: By definition,
$$f(R) = \{f(a) / a \in R\} \subseteq R'$$

IMS INSTITUTE OF MATHEMATICAL SCIENCES
Head Off.: A-31-34, 306, Top Floor, Jaina Extension, Dr. Mukherjee Nagar, Delhi-9.
Branch Off.: 87, First Floor (Back Side), Old Rajender Nagar Market, Delhi-110060
09999329111, 09999197625

Since $0 \in R$, $f(0) \in f(R)$

$\Rightarrow 0' \in f(R)$ $(\because f(0) = 0' \text{ in } R')$

clearly $f(R)$ is non-empty subset of R'

To show that $(f(R), +, \cdot)$ is a subring of R'.

Let $a', b' \in f(R)$

$\therefore \exists\ a, b \in R$ s.t

$f(a) = a'$, $f(b) = b'$.

Since $a-b \in R$, $ab \in R$

and hence $f(a-b), f(ab) \in f(R)$.

Now we have $a' - b' = f(a) - f(b)$

$= f(a-b)$ ($\because f$ is homo)

$\in f(R)$.

and $a'b' = f(a) \cdot f(b)$

$= f(ab)$. ($\because f$ is homo).

$\in f(R)$.

$\therefore f(R)$ is a subring of R'.

i.e the homomorphic image of the ring R is a subring of R'.

i.e the homomorphic image of a ring is a ring.

Theorem 3: Every homomorphic image of a commutative ring is a commutative ring.

Soln: Let $(R, +, \cdot)$ be a comm. ring and $(R', +, \cdot)$ be a ring.

Let $f: R \to R'$ be homo. and onto.

$\therefore R'$ is homomorphic image of R

i.e $R' = f(R)$.

~~Let $a', b' \in R'$~~

$\therefore \exists$ elements $a, b \in R$ s.t ..

$f(a) = a'$ &

$f(b) = b'$.

Since R is comm. ring

$\therefore \forall a, b \in R$

$\Longrightarrow ab = ba$

Now $a'b' = f(a) \cdot f(b)$

$= f(ab)$ ($\because f$ is homo)

$= f(ba)$.

$= f(b) f(a)$ ($\because f$ is homo)

$= b'a'$.

$\therefore R'$ is comm. ring.

Note: The converse of the above theorem need not be true. i.e if the homomorphic image of a ring R is commutative then the ring R need not be comm. ring.

For example:

Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} / a, b \in I \right\}$ be a ring

Then R is not a comm. ring

i.e Let $A = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 3 \\ 0 & 0 \end{pmatrix}$ be in R

then $AB \neq BA$.

Now we shall show that the mapping $f: R \to Z$ defined as

$$f\left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right\} = a \quad \text{——— (1)}$$

is an onto homo.

Let $x = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in R$

$y = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \in R$

We have $x+y = \begin{pmatrix} a+c & b+d \\ 0 & 0 \end{pmatrix}$

$xy = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$

Now $f(x+y) = a+c$

$= f(x)+f(y)$ (by ①)

$f(xy) = ac$

$= f(x).f(y)$ (by ①)

$\therefore f$ is homo.

Since for any $x \in Z$,

$\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \in R$ and

$f\left\{\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix}\right\} = x$ (Here $y \in Z$).

$\therefore f: R \to R'$ is onto.

Hence Z is homomorphic image of R.

Where Z is Comm. ring but

R is not Comm. ring.

Theorem: 4: The homorphic image of a ring with unity is also a ring with unity.

Soln:- Let $(R,+,.)$ be a ring with unity and $(R',+,.)$ be a ring.

Let $f: R \to R'$ be a homomorphism and onto.

$\therefore R'$ is the homomorphic image of R.

i.e $R' = f(R)$.

Let $a', b' \in R'$

$\therefore \exists$ elements $a, b \in R$ such that

$f(a) = a'$, $f(b) = b'$.

Since R is ring unity

$\therefore \forall a \in R, \exists 1 \in R$ s.t

$1 \cdot a = a = a \cdot 1$

Now since $1 \in R$ (unity in R).

We shall show that $f(1)$ is the unity in

We have

$a' \cdot f(1) = f(a) \cdot f(1)$

$= f(a \cdot 1)$ ($\because f$ is homo)

$= f(a)$ ($\because a \cdot 1 = a$ in R)

$= a'$

Similarly, $f(1) \cdot a' = a'$.

$\therefore \forall a' \in R', \exists f(1) \in R'$ s.t

$f(1) \cdot a' = a' \cdot f(1) = a'$

$\therefore R'$ is a ring with unity.

Note:- The converse of the need not be true i.e. if the homomorphic image of a ring R is ring with unity then the ring R need not be ring with unity.

for example:-

$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \middle/ a, b \in Z \right\}$ is a ring without unity. and Z is a ring with unity.

The mapping $f: R \to Z$ defined as $f\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\right\} = a$ is an onto homomorphism.

Note:- Even f is an isomorphism

(1) substitute 'isomorphism' for homomorphism in theorem ①. The same proof holds.

(ii) Substitute isomorphism for homomorphism in theorem ① and it is true. The same proof holds.

(iii) Substitute isomorphism onto for homomorphism onto in theorem ③ & ④ and it is true. The same proof holds.

* **Kernal of a homomorphism:-**

Let R, R' be two rings and $f: R \to R'$ be a homomorphism then Kernal of f, denoted by $\ker f$, is defined as

$$\ker f = \{x \in R \mid f(x) = 0', 0' \text{ is the +ve identity in } R'\} \subseteq R.$$

Note:- since $0 \in R$; $f(0) = 0'$ ($\because f$ is homo)

$\therefore 0 \in \ker f$.

$\therefore$ This shows that $\ker f$ is always non-empty i.e $\ker f \neq \phi$.

→ If f is a homomorphism of a ring R into a ring R' then $\ker f$ is an ideal of R.

Proof:- Let $f: R \to R'$ be the homomorphism.

Let $\ker f = \{x \in R / f(x) = 0', 0' \text{ is the identity in } R'\} \subseteq R$.

To prove that K is an ideal of R.

Since $0 \in R$ (The zero elt of R)

$\therefore f(0) = 0'$, The zero element of R'.

$\therefore 0 \in \ker f$

$\Rightarrow \ker f \neq \phi$

$\therefore \ker f$ is non-empty subset of R.

Let $a, b \in \ker f \subseteq R$, then $f(a) = 0'$ & $f(b) = 0'$.

Now we have

$f(a-b) = f(a) - f(b)$ ($\because f$ is homo)

$= 0' - 0'$

$= 0'$

$\therefore f(a-b) = 0' \Rightarrow \boxed{a-b \in \ker f}$

and $f(ar) = f(a) f(r)$

$= 0' f(r)$

$= 0'$ and,

$f(ra) = f(r) f(a)$

$= f(r) \cdot 0'$

$= 0'$

$\therefore ar \in \ker f, ra \in \ker f$.

Hence $\ker f$ is an ideal of R.

$\rightarrow$ If f is a homomorphism of a ring R into the R' then f is an into isomorphism if and only if $\ker f = \{0\}$

Sol: Let $f: R \rightarrow R'$ be the homomorphism.

Let f be an into homomorphism

i.e. f is 1-1 homomorphism.

Let $\ker f = \{x \in R / f(x) = 0'$, $0'$ is the identity in $R'\} \subseteq R$

Now we prove that

$\ker f = \{0\}$,

Let $a \in \ker f$ then $f(a) = 0'$

$\Rightarrow f(a) = f(0)$ $(\because f(0) = 0'$ in homo$)$

$\Rightarrow a = 0$ $(\because f$ is 1-1$)$

$\therefore$ 0 is the identity element in R which belongs to Kerf.

$\therefore \ker f = \{0\}$

Converse:-

Suppose $\ker f = \{0\}$

We prove that f is 1-1.

Let $a, b \in R$ and

$f(a) = f(b)$

$\Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a-b) = 0'$ $(\because f$ is homomorphism$)$

$\Rightarrow (a-b) \in \ker f$

$\Rightarrow a-b = 0$

$\Rightarrow a = b$

$\therefore f$ is 1-1

Note:- $\ker f = \{0\} \Leftrightarrow f$ is 1-1

$\rightarrow$ If U is an ideal of a ring R then the quotient ring $\frac{R}{U}$ is a homomorphic image of R.

(or)

Every quotient ring of a ring is a homomorphic image of the ring.

proof:- Given that U is an ideal of the ring R

$\therefore \frac{R}{U}$ is a quotient ring

i.e. Let $\frac{R}{U} = \{x+U / x \in R\}$ be a ring with respect $+^n$ and $\times^n$ cosets defined as

$(a+U) + (b+U) = (a+b) + U$

and $(a+U)(b+U) = ab + U$ where $a+U, b+U \in \frac{R}{U}$.

Let $f: R \to \frac{R}{U}$ be a mapping defined by

$f(a) = a+U$ for all $a \in R$ —— ①

First of we shall show that f is well-defined:-

for, $a, b \in R$, $a = b \Rightarrow$

$\Rightarrow a+U = b+U$

$\Rightarrow f(a) = f(b)$

$\therefore$ the mapping f is well-defined.

Now for $a, b \in R$

$\Rightarrow a+b \in R$

We have $f(a+b) = (a+b)+U$ (by ①)

$= (a+U)+(b+U)$

$= f(a)+f(b)$ (by ①).

and $f(ab) = ab+U$

$= (a+U).(b+U)$

$= f(a).f(b)$.

$\therefore f(ab) = f(a).f(b)$.

f is homomorphism.

Let $x+U \in \frac{R}{U}$ $\forall$ $x \in R$

For this $x \in R$, $f(x) = x+U$ (by ①)

$\therefore$ For each $x+U \in \frac{R}{U}$, $\exists$ $x \in R$ s.t

$f(x) = x+U$

$\therefore f$ is onto mapping.

Hence $f: R \to \frac{R}{U}$ is an onto homomorphism.

Note:– The mapping $f: R \to \frac{R}{U}$ such that $f(x) = x+U \; \forall x \in R$ is called Natural homomorphism (or) Canonical homomorphism.

* Fundamental theorem of homomorphism:–

Let R, R' be two rings and $f: R \to R'$ be an onto homomorphism with $\ker f$. Then R' is isomorphic to $\frac{R}{\ker f}$

i.e $R \simeq R' \Rightarrow \frac{R}{\ker f} \cong R'$

Proof: Let $f: R \to R'$ be a homomorphism and onto.

By definition of $\ker f$ is

$\ker f = \{ x \in R \,/\, f(x) = 0',\ 0' \text{ is the identity of } R' \} \subseteq R$

Let $\ker f = U$

We know that U is an ideal of R.

∴ The quotient ring $\frac{R}{U}$ is defined

Where $\frac{R}{U} = \{ x+U \,/\, x \in R \}$.

Given that $f: R \to R'$ is homomorphism and onto.

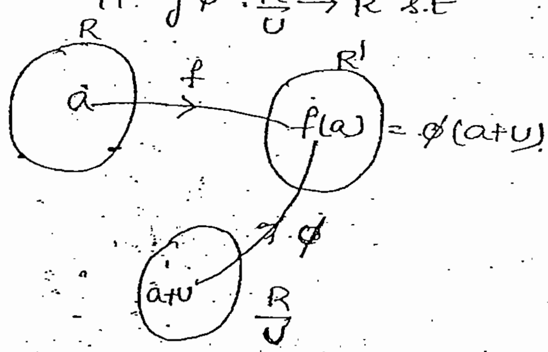
$\Rightarrow f(R) = R'$

$\Rightarrow R' = \{ f(a) \,/\, a \in R \}$.

Now we shall prove that $\frac{R}{U} \cong R'$

Now we define a mapping $\phi: \frac{R}{U} \to R'$ s.t

$\phi(a+U) = f(a) \; \forall a \in R$ ——— (1)



(i) Now we shall show that ϕ is well defined:-

Now $a+U,\ b+U \in \frac{R}{U}$

We have $a+U = b+U$

$\Rightarrow a-b \in U = \ker f$

$\Rightarrow f(a-b) = 0'$

$\Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \phi(a+U) = \phi(b+U)$ (by ①)

$\therefore \phi$ is well defined.

(ii) To prove ϕ is 1-1

For, $a, b \in R$, $a+U, b+U \in \frac{R}{U}$

Now we have $\phi(a+U) = \phi(b+U)$

$\Rightarrow f(a) = f(b)$ (by ①)

$\Rightarrow f(a) - f(b) = 0'$

$\Rightarrow f(a-b) = 0'$

$\Rightarrow a-b \in U = \ker f$

$\Rightarrow a+U = b+U$ ($\because U$ is an ideal)

$\therefore \phi$ is 1-1

(iii) To prove that ϕ is onto:-

Let $x \in R'$

Since $f: R \to R'$ is onto.

$\therefore \exists\ a \in R$ such that $f(a) = x$. —— ②

Now for $a+U \in \frac{R}{U}$ and $\phi(a+U) = f(a)$
$= x$.

$\therefore$ For each $a+U \in \frac{R}{U}$ $\exists\ x \in R'$
s.t $\phi(a+U) = x$
$\therefore \phi$ is onto.

(iv) To prove ϕ is homomorphism:-

For $a, b \in R$ is $a+U, b+U \in \frac{R}{U}$

We have $\phi((a+U)+(b+U)) = \phi((a+b)+U)$

$$= f(a+b) \text{ (by ①)}$$
$$= f(a)+f(b)$$
$$= \phi(a+U)+\phi(b+U),$$

and $\phi((a+U).(b+U))$

$$= \phi(ab+U) \text{ (by ①)}$$
$$= f(ab)$$
$$= f(a).f(b) (\because f \text{ is hom})$$
$$= \phi(a+U).\phi(b+U).$$

$\therefore \phi$ is homomorphism.

$\therefore \phi$ is isomorphism from $\frac{R}{U}$ onto R'

i.e., R' is an isomorphic image of $\frac{R}{U}$

i.e., $\frac{R}{U} \cong R'$

Note:- If $f: R \to R'$ is a homomorphism from a ring R onto R' and U is an ideal of R then $\frac{R}{U}$ is isomorphic to R'.

Ring of Endomorphisms of an Abelian group:-

Let $(G,+)$ be an abelian group. A homomorphism of G into itself is an endomorphism of G.

The set of all endomorphisms of G is denoted by $Hom(G,G)$.

Since the addition of two mappings is a mapping and the composition of two mappings is a mapping, we define addition $(+)$ and multiplication $(\cdot)$ of two endomorphisms as:

(i) $(f+g)(x) = f(x)+g(x)$

(ii) $(fg)(x) = f(g(x))$ for all $x \in G$.

Now we prove that $Hom(G,G)$ is a ring with respect to the addition and multiplication of endomorphisms.

Theorem: If $(G,+)$ is an abelian group then $Hom(G,G)$ is a ring under addition and composition of mappings.

Proof: $Hom(G,G)$ = the set of all endomorphisms of G.

If $f, g \in Hom(G,G)$ then

$f: G \to G$, $g: G \to G$ are homomorphisms

$\therefore f(x+y) = f(x)+f(y)$ and

$g(x+y) = g(x)+g(y) \;\forall\; x,y \in G$.

Now we show that $(\mathrm{Hom}(G,G), +)$ is an abelian group.

(1) Closure prop:

Let $f, g \in \mathrm{Hom}(G,G)$

$\Rightarrow f+g$ is a mapping from G to G.

For $x, y \in G$;

$(f+g)(x+y) = f(x+y) + g(x+y)$

$= (f(x)+f(y)) + (g(x)+g(y))$

$= (f(x)+g(x)) + (f(y)+g(y))$

$(\because f(x), f(y), g(x), g(y) \in G$ and G is abelian$)$.

$= (f+g)(x) + (f+g)(y)$.

$\therefore f+g$ is a homomorphism.

$\therefore f, g \in \mathrm{Hom}(G,G) \Rightarrow f+g \in \mathrm{Hom}(G,G)$.

So, addition of endomorphisms is a binary operation in $\mathrm{Hom}(G,G)$.

(2) Comm. prop:

For $x \in G$, $(f+g)(x) = f(x) + g(x)$

$= g(x) + f(x)$

$= (g+f)(x)$

$\therefore f, g \in \mathrm{Hom}(G,G) \Rightarrow f+g = g+f$.

$\therefore$ Addtion of endomorphisms is commutative.

(3) Asso. prop:

Let $f, g, h \in \mathrm{Hom}(G,G)$.

For $x \in G$; $((f+g)+h)(x) = (f+g)(x) + h(x)$

$= (f(x)+g(x)) + h(x)$

$= f(x) + (g(x)+h(x))$

$(\because f(x), g(x), h(x) \in G$ and G is a group$)$.

$= f(x) + (g+h)(x)$

$= (f+(g+h))(x)$

$\therefore f, g, h \in \mathrm{Hom}(G, G)$

$\Rightarrow (f+g)+h = f+(g+h)$.

$\therefore$ Addition is associative.

(4) Identity prop:

Define a mapping $O: G \to G$ by

$O(x) = e, \ \forall x \in G$.

Where 'e' is the identity in G.

For $x, y \in G$, $O(x+y) = e$ $\quad (\because x, y \in G \Rightarrow x+y \in G)$

$= e+e$

$= O(x)+O(y)$

$\therefore O$ is a homomorphism and hence $O \in \mathrm{Hom}(G, G)$.

For $f \in \mathrm{Hom}(G, G)$ and $\forall x \in G$;

$(f+O)(x) = f(x)+O(x)$

$= f(x)+e$

$= f(x)$

and $(O+f)(x) = f(x)$.

$\therefore O \in \mathrm{Hom}(G, G)$ such that

$O+f = f+O = f \ \forall f \in \mathrm{Hom}(G, G)$

(5) Inverse prop:

Let $f \in \mathrm{Hom}(G, G)$

Then $f: G \to G$ is a mapping.

Consider the mapping $(-f): G \to G$ defined by

$(-f)(x) = -f(x) \ \forall x \in G$

For $x, y \in G$, $(-f)(x+y) = -(f(x+y))$

$= -(f(x)+f(y))$

$(\because f$ is homomorphism$)$

$= -f(x) - f(y)$
$(\because f(x), f(y) \in G)$

$= (-f)(x) + (-f)(y).$

$\therefore -f$ is a homomorphism and hence $-f \in \mathrm{Hom}(G,G)$.

Also $\forall x \in G$, $(f+(-f))(x) = f(x) + (-f)(x)$
$= e$
$= o(x).$

$\therefore$ for $f \in \mathrm{Hom}(G,G)$ $\exists$ $-f \in \mathrm{Hom}(G,G)$ such that $f+(-f) = 0$.

Hence $(\mathrm{Hom}(G,G), +)$ is an abelian group.

Now we show that $(\mathrm{Hom}(G,G), \cdot)$ is semi-group.

closure prop:

for $f, g \in \mathrm{Hom}(G,G)$, the composite function of f and $g = fg$ is a mapping from G to G.

$\forall$ $x, y \in G$, $(fg)(x+y) = f(g(x+y))$
$= f(g(x)+g(y))$
$= f(g(x)) + f(g(y))$
$= (fg)(x) + (fg)(y).$

$\therefore fg$ is a homomorphism.

$\therefore f, g \in \mathrm{Hom}(G,G) \Rightarrow fg \in \mathrm{Hom}(G,G)$.

So, multiplication of two endomorphisms is a binary operation

Asso. prop:

Let $f, g, h \in \mathrm{Hom}(G,G)$

$\forall$ $x \in G$, $((fg)h)(x) = (fg)(h(x))$
$= f(g(h(x)))$
$= f((gh)(x))$
$= (f(gh))(x).$

$\therefore f, g, h \in Hom(G,G)$

$\Rightarrow (fg)h = f(gh)$

$\therefore$ multiplication is associative.

Distributive law:

Let $f, g, h \in Hom(G,G)$

$\forall x \in G, (f(g+h))(x) = f((g+h)(x))$

$= f(g(x) + h(x))$

$= f(g(x)) + f(h(x))$

$= (fg)(x) + (fh)(x).$

Similarly, $((g+h)f)(x) = (gf)(x) + (hf)(x).$

$\therefore f(g+h) = fg + fh$ and

$(g+h)f = gf + hf$

Hence $(Hom(G,G), +, \cdot)$ is a ring.

* Imbedding of Rings:-

A ring R is said to be imbedded in a ring R', if there exists an isomorphism of R into R' i.e. there exist a mapping $f: R \to R'$ such that (i) f is a homomorphism and (ii) f is 1-1

We also say that R' is an extension ring (or) over ring of R.

Note:- (1) Since f is an isomorphism of R into R', $f(R)$ is a subring of R' and further R and $f(R)$ are isomorphic rings.

② $f: R \to f(R)$ is an onto isomorphism and so $R \cong f(R)$.

③ Let R and R' be two rings.

A one-one homomorphism 'f' from R to R' is called an imbedding (embedding) mapping and in that case R' is called extension ring or over ring of R.

→ Every ring R can be imbedded in a ring with unity.

Proof:- Let R be any ring.

Let $R' = R \times Z = \{(a,m) / a \in R, m \in Z\}$

where Z denotes the ring of integers.

We now show that $R \times Z$ forms a ring with unity under addition and multiplication defined by $(r,m)+(s,n) = (r+s, m+n)$; $r,s \in R$, $m,n \in Z$ —— ①

$(r,m) \cdot (s,n) = (rs+ms+nr, mn)$ —— ②

Addition is well-defined:

let $(r,m) = (r',m')$ and $(s,n) = (s',n')$

then $r = r'$, $m = m'$ and $s = s'$, $n = n'$

$\Rightarrow r+s = r'+s'$; $m+n = m'+n'$

$\Rightarrow (r+s, m+n) = (r'+s', m'+n')$

Similarly we can show that multiplication is well-defined.

We shall show that $(R \times Z, +)$ is an abelian group:

(i) closure prop:-

By ①, $R \times Z$ is closed under $+^n$.

(ii) Associative prop :-

Let $(r,m),(s,n),(t,k) \in R\times Z$; $r,s,t\in R$, $m,n,k\in Z$

then $(r,m)+[(s,n)+(t,k)] = (r,m)+(s+t, n+k)$ (by ①)

$= (r+(s+t), m+(n+k))$ ($\because$ R & Z comm w.r.t. +)

$= ((r+s)+t, (m+n)+k)$

$= (r+s, m+n)+(t,k)$

$= [(r,m)+(s,n)]+(t,k)$

(iii) Existence of left identity :-

$\forall (r,m)\in R\times Z$, $\exists (0,0)\in R\times Z$

$r\in R, m\in Z$

s.t $(0,0)+(r,m) = (0+r, 0+m)$ (by ①)

$= (r,m)$.

$\therefore (0,0)$ is the left identity in $R\times Z$

(iv) Existence of left inverse :-

For each $(r,m)\in R\times Z$, $\exists (-r,-m)\in R\times Z$

s.t. $(-r,-m)+(r,m) = ((-r)+r, (-m)+m)$ (by ①)

$= (0,0)$

$\therefore (-r,-m)$ is the left inverse of (r,m) in $R\times Z$

(v) Commutative prop :-

Let $(r,m),(s,n)\in R\times Z$

then we have

$(r,m)+(s,n) = (r+s, m+n)$

$= (s+r, n+m)$ ($\because$ R & Z are comm. under $+^n$)

$= (s,n)+(r,m)$

$\therefore R\times Z$ is commutative under $+^n$

$\therefore (R\times Z, +)$ is an abelian group.

II We can easily show that $(R\times Z, \times)$ is a semi group.

III We can easily show that multiplication is distributive over the addition in $R\times Z$.

$\therefore (R\times Z, +, \times)$ is a ring.

IV Existence of $\times^{ve}$ identity:

since Z is a ring with unity

i.e $\forall\, m \in Z$, $\exists\, 1 \in Z$ s.t.

$1m = m1 = m$

Now for all $(r,m) \in R\times Z$, $\exists\, (0,1) \in R\times Z$

s.t. $(0,1)\times(r,m) = (0\cdot r + 1\cdot r + m(0), 1\cdot m)$ (by ②)

$= (r,m)$

similarly, $(r,m)\times(0,1) = (r,m)$.

$\therefore (0,1)$ will be unity in $R\times Z$.

$\therefore (R\times Z, +, \times)$ is a ring with unity.

Finally, we show that R can be embedded in $R\times Z$:

we now define a mapping:

$f: R \to R\times Z$ as $f(r) = (r,0)\ \forall\, r\in R$. ——— ③

To show that f is well-defined:

Now we have

$$r, s \in R \Rightarrow r = s$$
$$\Rightarrow (r,0) = (s,0)$$
$$\Rightarrow f(r) = f(s)$$

$\therefore f$ is well-defd.

To show that f is 1-1:

Now we have $f(r) = f(s)$; $r, s \in R$
$$\Rightarrow (r,0) = (s,0)$$
$$\Rightarrow r = s$$

Next we shall show that f is homo:

Let $r, s \in R$ then ③,
$$f(r) = (r, 0)$$
$$f(s) = (s, 0)$$

Since $r, s \in R \Rightarrow r+s \in R$ & $r.s \in R$

Now $f(r+s) = (r+s, 0)$ (by ③)
$$= (r+s, 0+0)$$
$$= (r,0) + (s,0)$$
$$= f(r) + f(s).$$

and $f(r.s) = (r.s, 0)$ (by ③)
$$= (rs + 0.s + 0r, 0.0)$$
$$= (r,0) \times (s,0) \quad \text{(by ②)}$$
$$= f(r) \times f(s).$$

$\therefore f$ is isomorphism of R into $R\times Z$.

And so R is imbedded in the ring $R\times Z$ with unity.

Note :- If R is any ring, not necessarily containing unity then its extension ring with unity is :-

$R\times Z = \{(r,m) / r\in R; m\in Z\}$.

* The field of quotients:

→ A ring R can be imbedded in a ring S if S contains a subset S' such that R is isomorphic to S'

If D is a commutative ring without zero divisors, then we shall see that it can be imbedded in a field F i.e there exists a field F which contains a subset D' isomorphic to D.

We shall construct a field F with the help of elements of D and this field F will contain a subset D' such that D is isomorphic to D'

This field F is called the "field of quotients" of D or simply the "quotient field" of D.

* Motivation for the construction of the quotient field:

We are all quite familiar with the ring I of Integers.

Also our familiar set Q of rational numbers is nothing but the set of quotients of the elements of I.

Thus $Q = \{\frac{p}{q} / p\in I, q\neq 0 \in I\}$

— If we identify the rational numbers

$$\cdots\cdots \frac{-3}{1}, \frac{-2}{1}, \frac{-1}{1}, \frac{0}{1}, \frac{1}{1}, \frac{2}{1}, \frac{3}{1} \cdots\cdots$$

with the integers $\cdots\cdots -3, -2, -1, 0, 1, 2, 3 \cdots\cdots$

then $I \subseteq Q$

Also $(Q, +, \cdot)$ is a field.

It is a smallest field containing I

Also if $\frac{a}{b}$ and $\frac{c}{d} \in Q$ then we have

(i) $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$

(ii) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

(iii) $\frac{a \cdot c}{bd} = \frac{ac}{bd}$

Taking motivation from these facts, we now proceed to construct the quotient field of an arbitrary integral domain.

We have the following theorem:

→ A commutative ring without zero divisors can be imbedded in a field.

(or)

Every integral domain can be imbedded in a field.

(or)

From the elements of an integral domain D, it is possible to construct a field F which contains a subset D' isomorphic to D.

(or)

An integral domain D can be embedded in a field F such that every element of F can be regarded as quotient of two elements of D.

Proof: Let D be an integral domain with atleast two elements.

Let us consider $S = \{(a,b) \mid a,b \in D ; b \neq 0\}$ then $S \neq \phi$ and $S \subset D \times D$.

$\forall (a,b), (c,d) \in S$

define a relation '$\sim$' on 'S' as

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$

we now prove that $\sim$ is an equivalence relation on S.

(1) for each $(a,b) \in S$,

we have $ab = ba$.

which implies that $(a,b) \sim (a,b)$.

(2) for $(a,b), (c,d) \in S$

we have $(a,b) \sim (c,d)$

$\Rightarrow ad = bc$

$\Rightarrow cb = da$

$\Rightarrow (c,d) = (a,b)$

(3) for $(a,b), (c,d), (e,f) \in S$

$(a,b) \sim (c,d)$, $(c,d) \sim (e,f)$

$\Rightarrow ad = bc$, $cf = de$

$\Rightarrow (ad)f = (bc)f$, $cf = de$

$\Rightarrow (af)d = b(de)$

$\Rightarrow (af)d = b(ed)$

$\Rightarrow (af)d = (be)d$

$\Rightarrow af = be$ $(\because d \neq 0)$

$\Rightarrow (a,b) \sim (e,f)$.

$\therefore \sim$ is an equivalence relation on 'S'.

the equivalence relation '$\sim$' partitions the set 'S' into equivalence classes which are identical or disjoint.

For $(a,b) \in S$,

let $\frac{a}{b}$ be denote equivalence class of (a,b)

then $\frac{a}{b} = \{(x,y) \in S \mid (x,y) \sim (a,b)\}$

i.e. $\frac{a}{b} = \{(x,y) \in S \mid (x,y) \sim (a,b) \Leftrightarrow xb = ya\}$

If $\frac{a}{b}, \frac{c}{d}$ are the equivalence classes of $(a,b), (c,d) \in S$.

then either $\frac{a}{b} = \frac{c}{d}$ or $\frac{a}{b} \cap \frac{c}{d} = \phi$

It is evident that $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$.

Let F denote the set of all the equivalence classes or the set of quotients then $F = \{\frac{a}{b} \mid (a,b) \in S\}$.

since D has at least two elements say $0, a \in D$,

we have quotients $\frac{0}{a}, \frac{a}{a} \in F$ and $\frac{0}{a} \neq \frac{a}{a}$.

$\therefore$ the set F has atleast two elements.

For $\frac{a}{b}, \frac{c}{d} \in F$; define addition $(+)$ and multiplication $(\cdot)$ as

(i) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and

(ii) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

since D is without zero divisors

$$b \neq 0, d \neq 0 \in D \Rightarrow bd \neq 0$$

so $\frac{ad+bc}{bd}, \frac{ac}{bd} \in F$

Now we prove that the $+^n$ and $\times^n$ defined above are well-defined.

Let $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{c}{d} = \frac{c'}{d'}$

Then $ab' = a'b$ and $cd' = c'd$ —— (I)

Now (I) $\Rightarrow ab'dd' = a'bdd'$ and $bb'cd' = bb'c'd$

$\Rightarrow ab'dd' + bb'cd' = a'bdd' + bb'c'd$

$\Rightarrow (ad+bc)\,b'd' = (a'd'+b'c')\,bd$

$\Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$

Also (I) $\Rightarrow ab'cd' = a'bc'd$

$\Rightarrow (ac)(b'd') = (a'c')(bd)$

$\Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$

$\therefore$ $+^n$ and $\times^n$ of quotients are well-defined binary operations on F.

we now prove that $(F,+,\cdot)$ is a field:

(1) For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f} = \frac{ad+bc}{bd}+\frac{e}{f}$

$$= \frac{(ad+bc)f+(bd)e}{(bd)f}$$

$$= \frac{a(df)+(cf+de)b}{b(df)}$$

$$= \frac{a}{b} + \frac{cf+de}{df}$$

$$= \frac{a}{b} + \left(\frac{c}{d}+\frac{e}{f}\right)$$

$\therefore$ addition is associative.

(2) For $\frac{a}{b}, \frac{c}{d} \in F$; $\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{bd}$

$$= \frac{bc+ad}{db}$$

$$= \frac{c}{d}+\frac{a}{b}$$

$\therefore$ addition is commutative.

(3) For $u \neq 0 \in D$ we have $\frac{0}{u} \in F$ such that

$$\frac{0}{u} + \frac{a}{b} = \frac{0b+ua}{ub} = \frac{ua}{ub} = \frac{a}{b} \;\forall\; \frac{a}{b} \in F.$$

$\therefore \frac{0}{u} \in F$ is the zero element.

(4). Let $\frac{a}{b} \in F$. Then $\frac{-a}{b} \in F$ such that

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-a)b}{b^2} = \frac{0}{b^2} = \frac{0}{u} \quad (\because 0u = 0b^2)$$

$\therefore$ every element in F has additive inverse.

(5). For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f} = \frac{ac}{bd}\cdot\frac{e}{f}$

$$= \frac{(ac)e}{(bd)f}$$

$$= \frac{a}{b}\cdot\frac{ce}{df} = \frac{a}{b}\left(\frac{c}{d}\cdot\frac{e}{f}\right)$$

$\therefore$ multiplication is associative.

(6) For $\frac{a}{b}, \frac{c}{d} \in F$, $\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\cdot\frac{a}{b}$.

$\therefore$ multiplication is commutative

(7) For $u \neq 0 \in D$ we have $\frac{u}{u} \in F$ such that

$$\frac{a}{b}\cdot\frac{u}{u} = \frac{au}{bu} = \frac{a}{b} \;\forall\; \frac{a}{b} \in F.$$

$\therefore \frac{u}{u} \in F$ is the unity element.

(8) Let $\frac{a}{b} \in F$ and $\frac{a}{b} \neq \frac{0}{u}$.

Then $au \neq 0$ which implies that $a \neq 0$ as $u \neq 0$.

$\therefore b \neq 0$ and $a \neq 0 \Rightarrow \frac{b}{a} \in F$.

$\therefore$ for $\frac{a}{b}\left(\neq \frac{0}{u}\right) \in F$ there exists $\frac{b}{a} \in F$ such that

$$\frac{a}{b}\cdot\frac{b}{a}=\frac{ab}{ba}=\frac{u}{u} \qquad (\because (ab)u=(ba)u)$$

$\therefore$ Every non-zero element in F has multiplicative inverse.

(9). For $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in F$; $\frac{a}{b}\cdot\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{cf+de}{df}$

$$=\frac{a(cf+de)}{b(df)}$$

$$=\frac{(acf+ade)(bdf)}{(bdf)(bdf)} \qquad \left[\because \frac{bdf}{bdf}=\frac{u}{u}\right]$$

$$=\frac{acf\,bdf+ade\,bdf}{bdf\,bdf}$$

$$=\frac{acf}{bdf}+\frac{ade}{bdf}$$

$$=\frac{ac}{bd}+\frac{ae}{bf}=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}$$

Similarly we can prove that

$$\left(\frac{c}{d}+\frac{e}{f}\right)\cdot\frac{a}{b}=\frac{c}{d}\cdot\frac{a}{b}+\frac{e}{f}\cdot\frac{a}{b}$$

$\therefore$ multiplication is distributive over addition.

In view of (1), (2), (3), (4), (5), (6), (7), (8) and (9) $(F,+,\cdot)$ is a field.

Now we have to prove that D is embedded in the field F, that is, we have to show that there exists an isomorphism of D into F.

Define the mapping $\phi: D\to F$ by

$$\phi(a)=\frac{ax}{x} \;\forall\; a\in D \text{ and } x(\neq 0)\in D.$$

$a, b\in D$ and $\phi(a)=\phi(b) \Rightarrow \frac{ax}{x}=\frac{bx}{x}$

$$\Rightarrow (ax)x=(bx)x$$

$$\Rightarrow (a-b)x^2=0$$

$$\Rightarrow a-b=0 \text{ since } x^2\neq 0.$$

$$\Rightarrow a=b$$

$\therefore \phi$ is one-one.

For $a, b\in D$; $\phi(a+b)=\frac{(a+b)x}{x}=\frac{(a+b)xx}{xx}$

$$= \frac{ax\,x + bx\,x}{xx}$$

$$= \frac{ax}{x} + \frac{bx}{x} = \phi(a) + \phi(b)$$

$$\phi(ab) = \frac{(ab)x}{x} = \frac{(ab)xx}{xx} = \frac{ax}{x} \cdot \frac{bx}{x} = \phi(a) \cdot \phi(b)$$

$\therefore \phi$ is a homomorphism.

Hence ϕ is an Isomorphism of D into F.

$\therefore$ the integral domain D is embedded in the field F.

Note 1: Every element in the field F is, in the form of a quotient of two elements in D. So, the field F is called "field of quotients of D".

2. The equivalence class of (a, b) is is also denoted as $[(a,b)]$ or $[a,b]$ or (a,b).

Then $[(a,b)] = [(c,d)] \Leftrightarrow ad = bc$,

$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$

$[(a,b)] \cdot [(c,d)] = [(ac, bd)]$

the zero element of $F = [(0,1)]$ and the unit element of $F = [(1,1)]$.

3. If D is the ring of integers then the field F, constructed in the above theorem, would be the field of rational numbers.

2003, Let R be the ring of all the real valued continuous functions on the closed unit interval. Show that $M = \{f \in R \mid f(\frac{1}{3}) = 0\}$ is maximal ideal of R.

Soln: Given that R be the ring of all the real valued continuous functions on the closed unit interval.

i.e, $R = \{f \mid f : [0,1] \to \mathbb{R}$ is continuous on $[0,1]\}$

where $\mathbb{R}$ denote the set of all real numbers.

Here R is a ring w.r.t compositions:

$(f+g)(x) = f(x) + g(x)$

$(fg)(x) = f(x)\, g(x)$ $\forall x \in [0,1]$ and $f, g \in R$

Now we shall show that

$M = \{f \in R \mid f(\frac{1}{3}) = 0\}$ is maximal ideal.

First of all we shall show that M is an ideal of R.

Now for this, first of all we observe that M is non-empty because the real valued function 'e' on $[0,1]$ defined by $e(x) = 0$ $\forall x \in [0,1]$.

$\therefore e \in M$.

$\therefore M$ is non-empty subset of R.

Now let $f, g \in M$ then $f(\frac{1}{3}) = 0$, $g(\frac{1}{3}) = 0$.

we have $(f-g)(\frac{1}{3}) = f(\frac{1}{3}) - g(\frac{1}{3})$

$= 0 - 0$

$= 0$

$\therefore f-g \in M$

$\therefore (M,+)$ is a subgroup of $(R,+)$

Let $f \in M$ and $h \in R$ then $f(1/3)=0$.

Now we have

$(fh)(1/3) = f(1/3)\, h(1/3) = 0 \cdot h(1/3) = 0$.

$\Rightarrow fh \in M$

Similarly $hf \in M$

$\therefore M$ is an ideal of R.

Finally we shall show that M is a maximal ideal of R.

Let us define a function $\theta : [0,1] \to \mathbb{R}$ such that $\theta(x) = 1 \;\; \forall x \in [0,1]$

then θ is a continuous function.

$\therefore \theta \in R$ (ring)

But $\theta \notin M$ as $\theta(1/3) = 1 \neq 0$

$\therefore M \neq R$.

Let U be any other ideal of R such that $M \subset U \subset R$ and $M \neq U$.

we need to show that $U = R$.

Since $M \subset U$ and $M \neq U$,

there exists a function $\lambda \in U$ such that

$\lambda \notin M$ i.e. $\lambda(1/3) \neq 0$

Let $\lambda(1/3) = c \neq 0$.

Let us define a function $\rho : [0,1] \to \mathbb{R}$ s.t. $\rho(x) = c \;\; \forall x \in [0,1]$.

then $\rho \in R$

Let $\psi = \lambda - \rho$ then $\psi(1/3) = \lambda(1/3) - \rho(1/3)$

$= c - c$

$= 0$.

$\Rightarrow \psi \in M$

$\Rightarrow \psi \in U$ as $M \subset U$

i.e $e = \lambda - \psi \in U$ $(\because \lambda, \psi \in U)$

If ϑ be a function from $[0,1]$ to $\mathbb{R}$

s.t $\vartheta(x) = \frac{1}{c}$, $(c \neq 0)$

then $\vartheta \in R$.

Now we have

$(\vartheta e)(x) = \vartheta(x)\, e(x)$

$= \frac{1}{c} \cdot c$

$= 1$

$= \theta(x)\ \forall x$.

$\Rightarrow \vartheta e = \theta$

Since $e \in U$, $\vartheta e \in U$

we find $\theta \in U$.

But θ is the unity of the ring R.

thus U is an ideal containing unity.

$\Rightarrow U = R$

Hence M is maximal ideal of the ring R.

Method (2) that M is maximal ideal can also be proved by using the fundamental theorem of homomorphism.

Let us define function

$\theta : R \longrightarrow \mathbb{R}$ such that

$\theta(f) = f(1/3) \quad \forall f \in R$ — (1)

where $\mathbb{R}$ = set of real numbers.

Then θ is a homomorphism as

$$\theta(f+g) = (f+g)(1/3)$$
$$= f(1/3) + g(1/3)$$
$$\boxed{\theta(f+g) = \theta(f) + \theta(g)}$$

&

$$\theta(fg) = (fg)(1/3)$$
$$= f(1/3)\, g(1/3)$$
$$\boxed{\theta(fg) = \theta(f) \cdot \theta(g)}$$

To check ontoness,

if $r \in \mathbb{R}$ ~~be any~~ element we can define another map $\phi : [0,1] \longrightarrow \mathbb{R}$ s.t

$$\phi(x) = r \quad \forall x \in [0,1].$$

Then ϕ being constant function will be continuous.

Thus $\phi = R$.

Also $\theta(\phi) = \phi(1/3)$, showing that ϕ is pre-image of r under θ.

i.e θ is onto.

Thus by fundamental theorem of homomorphism

$$\frac{R}{\operatorname{Ker}\theta} \cong \mathbb{R}$$

Now $f \in \operatorname{Ker}\theta \Leftrightarrow \theta(f) = 0$

$\Leftrightarrow f(1/3) = 0$

$\Leftrightarrow f \in M$.

$\Rightarrow \operatorname{Ker}\theta = M$

Hence $\frac{R}{M} \cong \mathbb{R}$, but being a field,

$\frac{R}{M}$ will be a field

i.e. M is maximal ideal of R.

($\because$ If R is a commutative ring with unity. An ideal M of R is maximal ideal of $R \Leftrightarrow \frac{R}{M}$ is a field.)

→ Let R be a commutative ring. An ideal P of R is a prime ideal iff for two ideals A, B of R, $AB \subseteq P \Rightarrow$ either $A \subseteq P$ or $B \subseteq P$.

Sol Let R be the commutative ring

Let P be a prime ideal of R and

Let A, B be two ideals of R s.t

$AB \subseteq P$.

suppose

$A \nsubseteq P$

$\therefore \exists$ some element $a \in A$ s.t $a \notin P$.

Since $AB \subseteq P$

In particular

$aB \subseteq P$ $(\because a \in A)$

$\Rightarrow ab \in P$ $\forall$ $b \in B$. — ①

Since P is prime ideal of R

we get either $a \in P$ or $b \in P$.

but $a \notin P$,

hence $b \in P$ $\forall$ $b \in B$.

$\Longrightarrow B \subseteq P$.

Conversely, suppose that

for two ideals A, B of R,

$AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$.

To P.T 'P' is a prime ideal of R.

Let $ab \in P$. — ①

Let A and B be ~~the~~ ideals generated by 'a' & 'b' then $A = (a)$, $B = (b)$.

If $x \in AB$ is any element then it is of the type

$x = a_1b_1 + a_2b_2 + \cdots\cdots + a_nb_n$; $a_i \in A$, $b_i \in B$.

$= (\alpha_1 a)(\beta_1 b) + (\alpha_2 a)(\beta_2 b) + \cdots + (\alpha_n a)(\beta_n b)$

for $\alpha_i, \beta_i \in R$ as $a_i \in A = (a)$,

$b_i \in B = (b)$.

Thus $x = (\alpha_1 \beta_1)(ab) + (\alpha_2 \beta_2)(ab) + \cdots \cdots + (\alpha_n \beta_n)(ab)$

$x = (\alpha_1 \beta_1 + \alpha_2 \beta_2 + \cdots + \alpha_n \beta_n)(ab)$

Since $ab \in P$, P is an ideal, all multiples of ab are in P.

Thus $x \in P$

i.e. $AB \subseteq P$

$\Rightarrow A \subseteq P$ or $B \subseteq P$

$\Rightarrow (a) \subseteq P$ or $(b) \subseteq P$

$\Rightarrow a \in P$ or $b \in P$

$\Rightarrow P$ is prime ideal of R.

→ Let R be a commutative ring with unity. If every ideal of R is prime, show that R is a field.

Sol: To show that R is a field, we need show that every non-zero element of R has multiplicative inverse. We first show that R is an integral domain.

Let $a, b \in R$ such that $ab = 0$

then $ab \in \{0\}$, which is an ideal of R and is, therefore, prime ideal.

$\Rightarrow a \in \{0\}$ or $b \in \{0\}$

$\Rightarrow a = 0$ or $b = 0$.

$\therefore R$ is an integral domain.

Let now $a \in R$ be any non-zero element and let $a^2R = \{a^2r / r \in R\}$

then it is easy to show that a^2R is an ideal of R.

$\therefore$ a^2R is an ideal of R and is therefore prime ideal.

Now $a \cdot a = a^2 = a^2 \cdot 1 \in a^2R$

$\Rightarrow a \in a^2R$

$\Rightarrow a = a^2b$ for some $b \in R$

$\Rightarrow a(1-ab) = 0$

$\Rightarrow 1-ab = 0$ as $a \neq 0$

$\Rightarrow ab = 1$

$\Rightarrow b$ is multiplicative inverse of a.

Hence R is a field

$\rightarrow$ Let R be a commutative ring with unity and let M be a maximal ideal of R such that $M^2 = \{0\}$. Show that if N is any maximal of R then $N = M$.

Soln: Let $m \in M$ be any element.

then $m \cdot m \in M^2 = \{0\}$

$\Rightarrow m^2 = 0 \in N$ (N is an ideal)

By known theorem, we know that every maximal ideal of R is prime.

$\therefore$ N is prime ideal.

$\Rightarrow m \in N$

$\Rightarrow M \subseteq N$

Thus $M \subseteq N \subseteq R$

Since M is maximal, $N = M$ or $N = R$

But N is maximal in R, thus $N \neq R$

Hence $N = M$.

→ Show that in a Boolean ring R, every prime ideal $P \neq R$ is maximal.

Sol: Let P be prime and I be any ideal such that $P \subseteq I \subseteq R$.

then $\exists$ some $x \in I$, such that $x \notin P$ and

as $x \in R$, $x^2 = x$

Let now, $y \in R$ be any element, then

$x^2 y = xy$

$\Rightarrow x(xy - y) = 0 \in P$ (P is an ideal)

$\Rightarrow xy - y \in P$ as $x \notin P$ and P is prime.

$\Rightarrow xy - y = p$ for some $p \in P$.

Then $y = xy - p \in I$

as $x \in I$, $y \in R$, $xy \in I$ and also $p \in P \subseteq I$,

$y \in I$

$\Rightarrow R \subseteq I$

$\Rightarrow I = R$

$\Rightarrow$

Definition: An ideal I of a commutative ring R is called semi prime ideal if $a^n \in I \Rightarrow a \in I$, for all $a \in R$.

Clearly then every prime ideal is semi prime.

For examples

→ Consider the ideal $I = \{6n / n \in \mathbb{Z}\}$ in the ring of integers.

Suppose $a^2 \in I$

Then a^2 is a multiple of 6.

i.e, $6 / a^2$

Since $2/6$, we find $2/a^2$

$\Rightarrow 2/a$ (as 2 is prime)

Similarly $3/a$.

$\Rightarrow 6/a$ as $g.c.d(2,3) = 1$

$\Rightarrow a \in I$.

Hence I is semi prime, but I is not prime as $2 \cdot 3 = 6 \in I$ but $2, 3 \notin I$.

→ Show that intersection of two prime ideals is a semi prime ideal and so is the intersection of two semi prime ideals.

→ Let R the ring of all real-valued continuous functions on the closed unit interval.

Show that (i) $M_1 = \{f \in R / f(1/5) = 0\}$

(ii) $M_2 = \{f \in R / f(2/3) = 0\}$ are maximal ideals of R.

(1)

If I feel unhappy, I do mathematics to become happy. If I am happy; I do mathematics to keep happy.

— PAUL TURAN —

Euclidean Domains and Unique Factorisation Domains

→ The division algorithm in the ring of integers is the motivation for the class of rings, namely, Euclidean rings.

Defn: An integral domain R is said to be a Euclidean ring or Euclidean domain if for every $a(\neq 0) \in R$ there is defined a non-negative integer $d(a)$ such that —

(i) $\forall a, b \in R$, $a \neq 0, b \neq 0$; $d(a) \leq d(ab)$ and

(ii) for any $a, b \in R$, $b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ where either $r = 0$ or $d(r) < d(b)$

Note:

1. For any $a(\neq 0) \in R$, $d(a) \geq 0$.
2. For the zero element 0 of R, $d(0)$ is not defined. However some authors defined $d(0) = 0$, integer.
3. The property (ii) in the above definition is called division algorithm.
4. From the above definition we note that $d : R - \{0\} \rightarrow Z$ is a mapping such that

(i) $d(a) \geq 0 \quad \forall a \in R-\{0\}$

(ii) $d(a) \leq d(ab)$ for all $a, b \in R-\{0\}$ and

(iii) there exist $q, r \in R$ so that $a = bq + r$ where either $r=0$ or $d(r) < d(b)$ for any $a \in R$, $b \in R-\{0\}$

Example (1): Show that the ring Z of integers is an Euclidean ring.

Sol: Given that the ring $(Z, +, \times)$ of integers is an integral domain.

Let us define the mapping $d: Z-\{0\} \to Z$ by $d(a) = |a| \quad \forall a \in Z-\{0\}$ ——— (1)

(i) Since $|a| > 0$,
we have $d(a) \geq 0 \quad \forall a \in Z-\{0\}$.

(ii) For $a \neq 0, b \neq 0$ in Z, $ab \neq 0$ in Z.

$$\begin{aligned}\therefore d(ab) &= |ab| \\ &= |a||b| \\ &\geq |a| \quad (\because |b| \geq 1) \\ &= d(a)\end{aligned}$$

$\therefore d(a) \leq d(ab)$

(iii) For $a, b \in Z, b \neq 0$; by division algorithm in integers,

$\exists\, q, r \in Z$ such that $a = bq + r$, where $0 \leq r < |b|$

i.e., $a = bq + r$, where $r = 0$ or $0 < r < |b|$

i.e., $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

$\therefore (Z, +, \times)$ is an Euclidean ring.

Example (2): Show that the ring of Gaussian integers is an Euclidean ring.

Sol: Given that $Z[i] = \{a + ib \mid a, b \in Z,\ i = \sqrt{-1}\}$ of Gaussian integers is an integral domain w.r.t '+' and '×'.

Let us define the mapping $d : Z[i]-\{0\} \to Z$

by $d(x+iy) = x^2+y^2 \ \forall \ x+iy \in Z[i]-\{0\}$.

i.e $d(x+iy) = |x+iy|$
$= x^2+y^2 \ \forall \ x+iy \in Z[i]-\{0\}$ ——— (1).

we have $x \neq 0$ or $y \neq 0$ and hence $x^2+y^2 \geq 1$.

$\therefore d(z) = d(x+iy) \geq 0 \ \forall \ z \in Z[i]-\{0\}$.

Let $z_1, z_2 \in Z[i]-\{0\}$ then we have

$z_1 = a+ib$; $z_2 = c+id$ where $a, b, c, d \in Z$ and
$a \neq 0$ or $b = 0$; $c \neq 0$ or $d \neq 0$.

$\therefore z_1 z_2 = (ac-bd)+i(ad+bc)$.

Now we have $d(z_1 z_2) = (ac-bd)^2+(ad+bc)^2$

$= (a^2+b^2)(c^2+d^2)$.

$\geq a^2+b^2 = d(z_1)$

$(\because c^2+d^2 \geq 1)$

$\therefore \boxed{d(z_1) \leq d(z_1 \cdot z_2).}$

Now we have

$$\frac{z_1}{z_2} = \frac{a+ib}{c+id}$$

$$= \frac{ac+bd}{c^2+d^2} + i\left[\frac{bc-ad}{c^2+d^2}\right]$$

$$\frac{z_1}{z_2} = p+iq \ (\text{say})$$

where $p = \frac{ac+bd}{c^2+d^2}$; $q = \frac{bc-ad}{c^2+d^2}$

are rational numbers.

Corresponding to the rational numbers p and q, we can find suitable integers p' and q' such that

$|p' - p| \leq \frac{1}{2}$ and $|q' - q| \leq \frac{1}{2}$

Let $t = p' + q'i$ then $t \in Z[i]$

and $\frac{z_1}{z_2} = \lambda$, where $\lambda = p + qi$

$\Rightarrow z_1 = \lambda z_2$

$= (\lambda - t) z_2 + t z_2$

$\boxed{z_1 = t z_2 + r}$ where $r = (\lambda - t) z_2$

NOW $z_1, z_2, t \in Z[i]$

$\Rightarrow z_1 - t z_2 \in Z[i]$

$\Rightarrow r \in Z[i]$.

$\therefore \exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$ where

$r = 0$, or

$d(r) = d[(\lambda - t) z_2]$

$= d[(p + qi) - (p' + q'i)] d(z_2)$

$= d[(p - p') + (q - q') i] d(z_2)$.

$= [(p - p')^2 + (q - q')^2] d(z_2)$.

$\leq \left[\frac{1}{4} + \frac{1}{4}\right] d(z_2)$

$= \frac{1}{2} d(z_2)$

$< d(z_2)$.

thus $\exists\ t, r \in Z[i]$ s.t $z_1 = t z_2 + r$

where $r = 0$ (or) $d(r) < d(z_2)$

<u>Note</u> :- from the deffnition of Euclidean domain, that $\exists$ a non-negative integer $d(a)$ for any $a \neq 0$, we mean, $\exists$ a function d from $R-\{0\}$ to $Z^+ \cup \{0\}$, where Z^+ is the set of +ve integers.

This function d is called Euclidean valuation on R.

Also the last condition in the definition is called Euclidean algorithm.

→ Every field is a Euclidean ring.

<u>Sol</u>: Let F be a field and F^* be the set of all non-zero elements of F.

Since F is a field, so F is an integral domain.

Define the mapping $d: F^* \to Z$ by

$d(a) = 0$ (zero integer) $\forall a \in F^*$ —— (1)

$\therefore d(a) \geq 0 \quad \forall a \in F^*$

Let $a, b \in F^*$

Then a, b and ab are non-zero elements of F.

$\therefore d(a) = 0$ and $d(ab) = 0$ (from (1))

$\therefore d(a) \leq d(ab)$.

Let $a \in F$ and $b \in F^*$

Now $a = a1$, where '1' is the unity element of F.

$= a(b^{-1}b)$

$= (ab^{-1})b$

$= (ab^{-1})b + 0$

where '0' is the zero element of the field F

$\therefore a = aq + r$ where $q = ab^{-1}$, $r = 0$.

Hence for $a \in F$, $b \in F^*$ there exist $q, r \in F$ such that $a = qb + r$ where $r = 0$

$\therefore$ F is an Euclidean ring.

Note: we can prove the above theorem by defining
$d : F^* \to \mathbb{Z}$ by $d(a) = 1$ (integer) $\forall a \in F^*$.

Q → The field Q of rational numbers with $d(a) = 1$ for all $a \neq 0 \in Q$ is a Euclidean domain. However, Q with $d(a) = |a|$ for all $a \neq 0 \in Q$, is not a Euclidean domain.

Sol: If $d(a) = 1$ $\forall a \neq 0 \in Q$, then Q is a Euclidean domain.

However, Q with $d(a) = |a|$ $\forall a \neq 0 \in Q$ is not a Euclidean domain,

Taking $a = \frac{3}{2}$, $b = \frac{2}{3}$; $\frac{3}{2} = \left|\frac{3}{2}\right| > 1 = \left|\frac{3}{2} \cdot \frac{2}{3}\right| = d(a \cdot b)$, a contradiction.

(A)

→ Show that $\mathbb{Z}[\sqrt{2}] = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\}$ is a Euclidean domain.

Sol^n: We know that $\mathbb{Z}[\sqrt{2}]$ is an integral domain with unity $1 = 1 + \sqrt{2}\cdot 0$.

Let us define a mapping

$$d : \mathbb{Z}[\sqrt{2}] - \{0\} \longrightarrow \mathbb{Z} \text{ by}$$

$$d(m+n\sqrt{2}) = |m^2 - 2n^2| \quad \forall\ m+n\sqrt{2} \in \mathbb{Z}[\sqrt{2}] - \{0\}$$

we have $m \neq 0$ or $n \neq 0$.

$\therefore$ $d(m+n\sqrt{2})$ is a +ve integer for each $m+n\sqrt{3} \in \mathbb{Z}[\sqrt{2}] - \{0\}$.

$\therefore$ $d(m+n\sqrt{2}) \geq 0$.

Now let: $a = m+n\sqrt{2} \neq 0$, $b = m_1 + n_1\sqrt{2} \neq 0$ in $\mathbb{Z}[\sqrt{2}]$, $m \neq 0$ or $n \neq 0$; $m_1 \neq 0$ or $n_1 \neq 0$.

~~then we have~~

$$ab = (mm_1 + 2nn_1) + (mn_1 + m_1 n)\sqrt{2}$$

and $$d(ab) = \left|(mm_1 + 2nn_1)^2 - 2(mn_1 + m_1 n)^2\right| \quad \text{(by defn)}$$

$$= \left|m^2 m_1^2 + 4n^2 n_1^2 - 2(m^2 n_1^2 + m_1^2 n^2)\right|$$

$$= \left|(m^2 - 2n^2)(m_1^2 - 2n_1^2)\right|$$

$$= |m^2 - 2n^2|\,|m_1^2 - 2n_1^2|$$

$$\geq |m^2 - 2n^2| \quad (\because |m_1^2 - 2n_1^2| \geq 1)$$

$$= d(a).$$

$\therefore$ $d(a) \leq d(ab)$.

Now we have ...

$$\frac{a}{b} = \frac{m+n\sqrt{2}}{m_1+n_1\sqrt{2}} = \frac{(m+n\sqrt{2})(m_1-n_1\sqrt{2})}{(m_1+n_1\sqrt{2})(m_1-n_1\sqrt{2})}$$

$$= \left(\frac{mm_1-2nn_1}{m_1^2-2n_1^2}\right) + \left(\frac{m_1n-mn_1}{m_1^2-2n_1^2}\right)\sqrt{2}$$

$$= p+q\sqrt{2}$$

where $p = \frac{mm_1-2nn_1}{m_1^2-2n_1^2}$ & $q = \frac{m_1n-mn_1}{m_1^2-2n_1^2}$ are rational numbers.

corresponding to the rational numbers p and q, we can find two integers p' and q' such that $|p'-p| \leq \frac{1}{2}$ and $|q'-q| \leq \frac{1}{2}$.

Let $t = p'+q'\sqrt{2}$.

Then $t \in Z[\sqrt{2}]$

we have $\frac{a}{b} = \lambda$, where $\lambda = p+q\sqrt{2}$

$$\Rightarrow a = \lambda b = (\lambda - t)b + tb$$

$$= tb + r, \text{ where } r = (\lambda - t)b$$

Now $a, b, t \in Z[\sqrt{2}]$

$$\Rightarrow a - tb \in Z[\sqrt{2}]$$

$$\Rightarrow r \in Z[\sqrt{2}]$$

$\therefore$ $\exists$ $t, r \in Z[\sqrt{2}]$ such that

$a = tb + r$; where $r = 0$ (or)

$$d(r) = d\{(a-t)b\}$$
$$= d\{(p+q\sqrt{2})-(p'+q'\sqrt{2})\}\, d(b)$$
$$= d\{(p-p')+(q-q')\sqrt{2}\}\, d(b)$$
$$= |(p-p')^2 - 2(q-q')^2|\, d(b)$$
$$\leq |(p-p')^2 + 2(q-q')^2|\, d(b)$$
$$\leq \left(\frac{1}{4}+\frac{2}{4}\right) d(b)$$
$$= \frac{3}{4}\, d(b)$$
$$< d(b).$$

$\therefore$ $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

H.W. $\rightarrow$ Show that $\mathbb{Z}[\sqrt{3}] = \{m+n\sqrt{3} : m, n \in \mathbb{Z}\}$ is a Euclidean domain.

→ Every Euclidean ring is a principal ideal ring.

(or)

Every ideal of an euclidean ring is a principal ideal.

<u>proof</u> Let R be an euclidean ring.

Let U be an ideal of R.

To prove that U is a principal ideal.

Let $U=\{0\}$, where '0' $\in R$.

Then $U=\{0\}$ is the ideal generated by '0' $\in R$.

$\therefore U$ is a principal ideal of R.

Let $U \neq \{0\}$ then U contains non-zero elts.

Then $\exists\, x \in U (\subseteq R)$ and $x \neq 0$ so that the set $\{d(x) / x \neq 0\}$ is a non-empty set of non-negative integers.

$\therefore$ By well ordering principle there exists $b \neq 0$ in U s.t $d(b) \leq d(x)$ where $x \neq 0 \in U$.

Now we prove that $U = \langle b \rangle$.

Let $a \in U$

By division algorithm, $\exists\, q, r \in R$ s.t $a = bq + r$ where $r = 0$ (or) $d(r) < d(b)$.

Since $b \in U$, $q \in R \Rightarrow bq \in U$ ($\because U$ is an ideal)

Since $a \in U$, $bq \in U \Rightarrow a - bq = r \in U$.

if $r \neq 0$ then $d(r) < d(b)$ which contradiction to the fact $d(b) \leq d(x)$ $\forall x \neq 0 \in U$.

$\therefore r = 0$ and hence $a = bq$.

$\therefore U = \{bq / q \in R\} = \langle b \rangle$ is the principal ideal generated by 'b' $(\neq 0)$ for U.

Hence every ideal U of R is a principal ideal.

$\therefore$ R is a principal ideal ring.

Note: ① If U is an ideal of euclidean ring R then U is a principal ideal of R so that

$U = \langle b \rangle$

$= \{bq / q \in R\}$.

② The ~~converse~~ of the above theorem need not be true.

Ex:— $R = \left\{ a + b\left(\frac{1+\sqrt{19}\,i}{2}\right) / a, b \in Z \right\}$, the ring of complex numbers is a ~~principal~~ ideal ring but not Euclidean. (It will clear in UFD)

→ Every Euclidean ring possesses unity element.

Sol: Let R be an Euclidean ring.

$\therefore$ R is a principal ideal ring.

$\therefore$ R is an ideal generated by some element c of the ring R so that

$R = (c) = \{cq / q \in R\}$

$\therefore c \in R \Rightarrow c = ce$ for some $e \in R$.

We now prove that $e \in R$ is the unity.

Let $x \in R$. Then $x = cd$ for some $d \in R$

Now $xe = (cd)e = (dc)e = d(ce) = dc = cd = x$ ($\because$ R is I.D)

$\therefore xe = x \ \forall x \in R$.

Hence $e \in R$ is the unity element.

Corollary: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ are principal ideal domains.

Divisibility:– Let R be a commutative ring and $a, b \in R$, if $\exists\, q \in R$ s.t $b = aq$ then we say that 'a' divides 'b'.

Note: ① If 'a' divides 'b' then $a|b$.

② if a does not divide 'b' then $a \nmid b$.

③ If 'a' divides 'b' then we say that 'a' is a divisor of 'b' or 'a' is a factor of 'b'.

④ For $a, 0 \in R$.
we have $0 = a \cdot 0$.
Therefore every element $a \in R$ is a divisor or factor of '0'.

⑤ $a, b \in R$ and $a|b \Leftrightarrow b = aq$ for some $q \in R$.

For example:

(i) In the ring $\mathbb{Z}$ of integers,
$3|15$ and $3 \nmid 7$.

(ii) In the ring $\mathbb{Q}$ of rational numbers
$3|7$ because there exists $\frac{7}{3} \in \mathbb{Q}$
so that $7 = 3 \cdot \frac{7}{3}$.

→ If R is a commutative ring with unity and $a, b, c \in R$ then (1) $a|a$ (2) $a|b, b|c \Rightarrow a|c$
(3) $a|b \Rightarrow a|bx$ $\forall\, x \in R$ and (4) $a|b, a|c \Rightarrow a|bx+cy$ $\forall\, x, y \in R$.

proof: (1) If $1 \in R$ is the unity element then we have $a = a1$.

Therefore $a|a$.

(2) $a|b \Rightarrow b = aq_1$ for some $q_1 \in R$

$b|c \Rightarrow c = bq_2$ for some $q_2 \in R$

$\therefore c = bq_2 = (aq_1)q_2 = a(q_1 q_2) = aq$

where $q = q_1 q_2 \in R$

$\therefore a|c$.

(3) $a|b \Rightarrow b = aq$ for some $q \in R$

Now $bx = (aq)x = a(qx) = aq'$

where $q' = qx \in R$

$\therefore a|bx$.

(4) $a|b \Rightarrow a|bx \Rightarrow bx = aq_1$ for some $q_1 \in R$

$a|c \Rightarrow a|cy \Rightarrow cy = aq_2$ for some $q_2 \in R$

Now $bx + cy = aq_1 + aq_2$

$= a(q_1 + q_2)$

$= aq$, where $q = q_1 + q_2 \in R$

$\therefore a|bx+cy$

Note: $a|b,\ a|c \Rightarrow a|b+c$ and $a|b-c$.

Units:

Let R be a commutative ring with unity element 1. An element $a \in R$ is a unit in R if $\exists$ an element $b \in R$ such that $ab = 1$.

In other words units of R are those elements of R which possess multiplicative inverse.

finally, be careful not to confuse a unit with the unit element or the unity element of the ring. There may be more than one units in a ring but the unity element is always unique. Of course the unity element is also one of the units.

Examples:

(1) ± 1 are the units in I (all integers).
($\because$ These are only the inversible elements of the ring of integers).

(2) $\pm 1, \pm i$ are the units in $Z[i] = \{a + ib / m, n \in Z\}$ where $i = \sqrt{-1}$.

($\because 1(1) = 1$, $(-1)(-1) = 1$ and $i(-i) = 1$)

→ $a \in R$ is a unit of $R \Rightarrow ab = 1$ for some $b \in R$, so $b \in R$ is also a unit of R.

→ If a, b are two units in R, then ab is also a unit in R.

Examples:

(1) In the ring Z of integers, we have $1 \cdot 1 = 1$ and $(-1)(-1) = 1$ only.
1 and -1 are the only units in Z.

(2) If R is a field then every non-element of R has multiplicative inverse.

So, every non-zero element of a field is unit.

(3) $3+2\sqrt{2}$ is a unit in the domain

$$\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \,/\, a,b \in \mathbb{Z}\}$$

For, $3,-2 \in \mathbb{Z}$ we have

$3-2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ so that $(3+2\sqrt{2})(3-2\sqrt{2})=1$

when $1 \in \mathbb{Z}[\sqrt{2}]$ is the unity element.

Also every integral power of $3+2\sqrt{2}$ is also a unit of $\mathbb{Z}[\sqrt{2}]$.

Thus $\mathbb{Z}[\sqrt{2}]$ has infinite number of distinct units.

→ Let a,b be two non-zero elements of an Euclidean ring R. Then (1) if b is a unit in R, $d(ab)=d(a)$ and (2) if b is not a unit in R, $d(ab)>d(a)$.

Proof: By definition of Euclidean ring,

$$d(ab) \geq d(a) \quad \text{——— (1)}$$

(1) b is a unit in $R \Rightarrow$ there exists $c \in R$ such that $bc=1$.

By the definition of Euclidean ring,

$$d((ab)c) \geq d(ab).$$

i.e, $d(a(bc)) \geq d(ab)$

i.e, $d(a1) = d(a) \geq d(ab)$ ——— (2)

from (1) and (2) : $d(ab) = d(a)$.

(2) Let 'b' be not a unit in R.

$a \neq 0$, $b \neq 0 \in R$ and R is integral domain

$\Rightarrow ab(\neq 0) \in R$

By the division algorithm, there exist $q, r \in R$ such that $a = q(ab) + r$ where either $r = 0$ or $d(r) < d(ab)$.

If $r = 0$, $a = q(ab)$ i.e, $a = a(qb)$

i.e., $a(1 - qb) = 0$

Since R is an integral domain and $a \neq 0$ we have $1 - qb = 0$ i.e., $qb = 1$ which implies that b is a unit in R.

$\therefore r \neq 0$ and hence $d(r) < d(ab)$

i.e., $d(a - q(ab)) < d(ab)$

i.e., $d(a(1 - qb)) < d(ab)$

But $d(a(1 - qb)) \geq d(a)$ by the definition.

$\therefore d(a) \leq d(a(1 - qb)) < d(ab)$

Hence $d(a) < d(ab)$.

→ A non-zero element 'a' of a Euclidean ring R is unit $\Leftrightarrow d(a) = d(1)$.

Sol Let $a (\neq 0) \in R$ be a unit in R

$\therefore \exists\ b \in R$ s.t $ab = 1$.

$\therefore d(1) = d(ab) \geq d(a)$. (by the definition of Euclidean ring) — ①

Also $d(1a) \geq d(1)$ (by defn of ED)

$\Rightarrow d(a) \geq d(1)$ — ②

$\therefore$ from ① and ② we have $d(a) = d(1)$.

Conversely, let $d(a) = d(1)$
T.P.T $a (\neq 0)$ is an unit in R

If possible let a is not unit in R

then $d(a) = d(1a) > d(1)$ (by definition of ED)

$\Rightarrow d(a) > d(1)$.

This is a contradiction.

Hence 'a' must be a unit in R.

Associates :-

Let R be a commutative ring with unity. An element $a \in R$ is said to be an associate of $b \in R$ if $a = bu$ where u is a unit in R.

Note :- ① The relation of being associates is an equivalence relation in R. So if $a \in R$ is an associate of $b \in R$, by the property of symmetry, $b \in R$ is an associate of $a \in R$.

Therefore two elements $a, b \in R$ are associates in R if $a = bu$ where u is unit in R.

② If a, b associate in R then $a = bu$ where u is unit in R. Therefore, $d(a) = d(bu) = d(b)$

③ If a is an unit of the ring R and 1 is the unity element then $a = 1a$, so the unity element '1' is an associate of the unit 'a'.

For example : ① In the ring Z of integers the units are $1, -1$ only.

for $a \in Z$, we have $a = a \cdot 1$ &
$a = (-a)(-1)$ only.

Therfore $a \in Z$ has only two associates $a, -a$.

② In the ring $Z_6 = \{0, 1, 2, 3, 4, 5\}$ of integers modulo 6, the units are $1, 5$ only.

for $2 \in Z_6$, we have $2 \equiv 2 \cdot 1 \pmod 6$

and $2 \equiv 4 \cdot 5 \pmod 6$

$\therefore$ 2 has two associates 2 and 4.

(3) 1 and $-i$ are associates in $Z[i]$,
since $1 = (-i)(i)$, i being unit in $Z[i]$.

(4) $2+3i$ and $2i-3$ are associates,
since $2i-3 = (2+3i)i$,
i being a unit in $Z[i]$.

→ If a, b are two non-zero elements of an integral domain R with unity then a, b are associates in R if and only if a/b and b/a.

Sol: Let a, b be associates in R.

Since 'a' is an associate of b,

$a = bu$ for some unit $u \in R$.

$\therefore b/a$.

Since 'b' is an associate of 'a',

$b = au'$ for some unit $u' \in R$.

$\therefore a/b$.

Conversely, let a/b and b/a.

$\therefore b = aq_1$ and $a = bq_2$ for some $q_1, q_2 \in R$.

$\therefore b = aq_1 = (bq_2)q_1 = b(q_2 q_1) = 0$

$\Rightarrow b(1-q_2 q_1) = 0$

Since $b \neq 0$ and R is an integral domain.

we have

$1 - q_2 q_1 = 0$

$\Rightarrow q_2 q_1 = 1$

$\therefore q_2$ is a unit in R.

$\therefore a = bq_2$ where q_2 is a unit in R.

Hence a, b are associates in R.

→ Greatest Common Divisor:

Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $d \in R$ is called a highest common factor (h.c.f) or a greatest common divisor (g.c.d) of a and b if (i) d/a and d/b

(ii) whenever $c \neq 0 \in R$ such that c/a and c/b, then c/d.

g.c.d of a and b is denoted by (a, b).

Least Common Multiple: Let R be a commutative ring and a, b be any two non-zero elements of R. A non-zero element $c \in R$ is called a least common multiple (l.c.m) of a and b, if

(i) a/c and b/c

(ii) whenever $x \neq 0 \in R$ is such that a/x and b/x, then c/x.

l.c.m of a and b is denoted by $[a, b]$.

Note: Any two non-zero elements of a ring may or may not have a g.c.d (l.c.m). They may even have more than one g.c.d (l.c.m).

Head Off.: A-31-34, 306 Top Floor, Jaina Extension, Dr. Mukherjee Nagar, Delhi-9
Branch Off.: 27, First Floor Back Side, Old Rajinder Nagar, New Delhi-110060
09999329111, 09999197625

Examples:

(1) In $\mathbb{Z}$, 2 is a g.c.d of 4 and 6. Also -2 is a g.c.d of 4 and 6. further 12 is an l.c.m. of 4 and 6. Similarly -12 is also l.c.m of 4 and 6.

(2) In the ring E of even integers, 4 and 6 do not have a g.c.d;
Notice that $2 \in E$ is not a g.c.d of 4 and 6,
Since $2.2 = 4 \Rightarrow 2/2$ in E, but $2.3 = 6 \Rightarrow 2 \nmid 6$ $(\because 3 \notin E)$

Similarly, 4 and 6 do not have a l.c.m.
Notice that $12 \in E$ is not a l.c.m. of 4 and 6,
since $4 \nmid 12$ in E; $(\because 12 = 4 \cdot 3$ and $3 \notin E)$.

(3) In $\mathbb{Z}$, 6 is a g.c.d of 18 and 48.
Another g.c.d of 18, 48 is -6.

(4) Consider the ring:
$\mathbb{Z}_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$ of residue classes modulo 12;
consider $\bar{6}, \bar{8} \in \mathbb{Z}_{12}$
since $\bar{6} = \bar{3}.\bar{2}$ and $\bar{8} = \bar{4}.\bar{2}$;
$\bar{2}$ is a common divisor of $\bar{6}, \bar{8}$.
If $\bar{x} \in \mathbb{Z}_{12}$ and $\bar{x} \neq \bar{0}$ then $\bar{x}/\bar{6}$; $\bar{x}/\bar{8}$.
$\Rightarrow \bar{x}/\bar{8} - \bar{6}$ i.e, $\bar{x}/\bar{2}$
$\therefore$ 2 is a g.c.d of $\bar{6}$ and $\bar{8}$.
Again $\bar{6} = \bar{10}.\bar{3}$ and $\bar{8} = \bar{10}.\bar{2}$.
$\Rightarrow \bar{10}/\bar{6}$ and $\bar{10}/\bar{8}$.
Let $\bar{x} \neq \bar{0} \in \mathbb{Z}_{12}$ be such that $\bar{x}/\bar{6}$ and $\bar{x}/\bar{8}$

Then $\bar{x} \mid (\bar{2}\cdot\bar{8}-\bar{6})$ i.e. $\bar{x} \mid \overline{10}$

- Thus $\overline{10}$ is also a g.c.d of $\bar{6}$ and $\bar{8}$

Now we show that $\bar{6}$ and $\bar{8}$ have no l.c.m.

Let $\bar{x}$ be an l.c.m of $\bar{6}$ and $\bar{8}$.

Then $\bar{6}/\bar{x}$ and $\bar{8}/\bar{x}$

Now $\bar{6}/\bar{x} \Rightarrow \bar{x} = \bar{6}\cdot\bar{y}$, for some $\bar{y} \in Z_{12}$

$\Rightarrow \bar{x} = 0$ or $\bar{6}$

$\Rightarrow \bar{x} = \bar{6}$ ($\because$ l.c.m. is never zero)

It follows that $\bar{8}/\bar{6}$ and so $\bar{6} = \bar{8}\cdot\bar{z}$, for some $z \in Z_{12}$

Consequently, $\bar{6} = \bar{8}\cdot\bar{z}$ impossible.

Hence $\bar{6}$ and $\bar{8}$ have no l.c.m in Z_{12}.

Note: If d_1, d_2 are two g.c.d.s of a, b then by the definition d_1/d_2 and d_2/d_1.

$\therefore d_1, d_2$ are associates of the ring

Thus in case of a g.c.d of a, b exists then it is unique apart from the distinction between associates.

In the above examples ①, ③ and ④

$2, -2$ are associates in Z

$12, -12$ are associates in Z

③ & ④ $\bar{6}, -\bar{6}$ and $\bar{2}, \overline{10}$ are associates in Z and Z_{12} respectively.

→ In the ring $Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$, show that

(i) g.c.d $(\bar{4}, \bar{6}) = \bar{2}$ and $\bar{6}$

(ii) l.c.m $(\bar{4}, \bar{6}) = \bar{6}$

(iii) l.c.m $(\bar{3}, \bar{6}) = \bar{2}$ and $\bar{6}$.

→ Show that in Z_{20}, g.c.d. $(\bar{9}, \bar{18}) = \bar{9}$ and l.c.m. $(\bar{9}, \bar{18}) = \bar{18}$.

→ In the Euclidean ring R two elements 'a' and 'b' are said to be <u>relatively prime</u> if their greatest common divisor is a unit of R.

Since any associate of g.c.d is a g.c.d. and ~~the~~ unity element 1 is an associate of a unit.

a, b are relatively prime ⟺ (a,b) = unit of R.

$\Leftrightarrow (a,b) = 1$

$\Leftrightarrow ax + by = 1$ for some $x, y \in R$.

→ Let 'a' be non-zero element of an integral domain R with unity element. If $b \in R$ is a divisor of 'a' but not an associate of 'a' then 'b' is a proper divisor of 'a'.

'b' is a <u>proper divisor</u> of 'a'.

$\Rightarrow a = bd$ where d is not a unit.

For any non-zero element 'a' of R, the units and associates of 'a' are divisors.

These are called <u>improper divisors</u> of 'a'.

<u>Irreducible Element</u>: Let R be a commutative ring with unity.

A non-zero and non-unit $p \in R$ is said to be an irreducible element, if $p = ab$ implies that either a or b is a unit; $a, b \in R$.

 9(iv)

Note: It may be observed that $p \in R$ is not irreducible, if there exists a pair of elements $a, b \in R$ such that $p = ab$, where a and b are both non-unit elements of R.

Prime Elements: Let R be a commutative ring with unity. A non-zero, non-unit element $p \in R$ is called a prime element if $p \mid ab$ $(a, b \in R)$ implies that either $p \mid a$ or $p \mid b$.

Ex: ①. In the ring Z of integers the units are 1 and -1 only. If $p \in Z$ and $p \neq \pm 1$ and $p = p \cdot 1$ or $p = (-p)(-1)$ only then p is prime element in Z.

②. In the ring $Z[i]$ of Gaussian integers $1+i$ is a prime element.

Note:
① It may be observed that $p \in R$ is not prime, if there exists a pair of elements, $a, b \in R$ such that $p \mid ab$, but $p \nmid a$ and $p \nmid b$.

② Irreducible and prime elements in a commutative ring with unity are always non-zero and non-unit elements.

③ In the ring Z of integers, every prime number is both a prime element and irreducible element.

* Polynomial Rings and Division Algorithm *

"very early in our mathematical education in fact in junior high school or early in high school itself – we are introduced to polynomials. For a seemingly endless amount of time we are drilled, to the point of utter boredom, in factoring them, multiplying them, dividing them, simplifying them. Facility in factoring a quadratic becomes confused with genuine mathematical talent."

I.N. HERSTEIN, Topics in Algebra

Later, at the beginning college level, polynomials make their appearance in a somewhat different setting. Now they are functions, taking on values and we become concerned with their continuity, their derivatives, their integrals, their maxima and minima.

We too shall be interested in polynomials but from neither of the above view points. To us polynomials will simply be elements of a certain ring and we shall be concerned with algebraic properties of thi

Let F be a field. By the ring of polynomials in the indeterminate, x, written as $F[x]$, we mean the set of all symbols $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, where n can

be any non-negative integer and where the co-efficients $a_1, a_2, \ldots, a_n$ are all in F. In order to make a ring out of F[x], we must be able to recognize when two elements in it are equal, we must be able to add and multiply elements of F[x] so that the axioms defining a ring hold true for F[x].

Note: we could avoid the phrase "the set of all symbols" used above by introducing an appropriate apparatus of sequences but it seems more desirable to follow a path which is some what familiar to most readers.

Polynomial: Let R be a ring. Let $x \notin R$ where x is indeterminate. The expression of the form

$$f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n. \quad \forall a_i \in R.$$

and n is a non-negative integer is called a polynomial in x over R. Here $a_i x^i$ are called the terms of the polynomial and a_i are called the coefficients of the terms of the polynomial.

→ If n is the largest non-negative integer such that $a_n \neq 0$ then 'a_n' is called the leading coefficient.

Ex-①:

$$5x^0 - 7x^2 - 8x^4 - \frac{3}{2}x^5.$$

This is called a polynomial in x. Since the coefficients are rationals.

∴ It is a polynomial in 'x' over the field of rationals.

Ex-(2): $5x^2 + \pi x^3 + 7x^4$.

This is polynomial over the field of reals.

Equal polynomials:

→ Let $f(x) = a_0x^0 + a_1x^1 + \dots + a_ix^i + \dots + a_mx^m$ and $g(x) = b_0x^0 + b_1x^1 + \dots + b_ix^i + \dots + b_nx^n$ be two polynomials over R.

$f(x) = g(x)$ iff the coefficients of x are same on both sides except zero coefficients.

i.e., $f(x) = g(x)$ iff $a_i = b_i \ \forall i \geq 0$ except zero coefficient.

Ex: $5x^0 + 7x^3 + 9x^7$ is a polynomial over integers.

∴ It is a polynomial in x over the ring of integers.

Again $5x^0 + 0x^1 + 0x^2 + 7x^3 + 0x^4 + 0x^5 + 0x^6 + 9x^7$ —— (1)

These polynomials are equal.

(∵ Coefficients of like powers of x on both sides are equal).

→ **Monic polynomial:** A polynomial is called monic polynomial when the leading coefficient is the unity element.

→ **Ring of Polynomials:**

Let R be a ring. The ring of polynomials in the indeterminate 'x' denoted as $R[x]$, is defined as the set.

$$R[x] = \left\{ f(x) = a_0x^0 + a_1x^1 + a_2x^2 + \dots + a_nx^n \,/\, a_i \in R \text{ and } n \geq 0 \in \mathbb{Z} \right\}.$$

We shall give $R[x]$ a ring structure as follows:

Let $f(x) = a_0x^0 + a_1x^1 + \dots\dots + a_nx^n \in R[x]$

$g(x) = b_0x^0 + b_1x^1 + \dots\dots + b_mx^m \in R[x]$

we define:

Sum: $f(x) + g(x) = (a_0+b_0)x^0 + (a_1+b_1)x^1 + \dots\dots + (a_i+b_i)x^i + \dots\dots$

$= c_0 + c_1x + c_2x^2 + \dots\dots + c_ix^i + \dots$ —— (A)

Product:

$f(x)\,g(x) = c_0 + c_1x + c_2x^2 + \dots\dots + c_ix^i + \dots\dots$ —— (B)

where $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0$

$c_i = a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \dots\dots + a_{i-1}b_1 + a_ib_0$

→ It is easy to verify that $R[x]$ is a ring w.r.t the compositions given by (A) and (B), where the additive identity is $0 = 0 + 0.x + 0x^2 + \dots$ and the additive inverse of $f(x)$ is $-f(x) = -a_0 - a_1x - a_2x^2 - \dots\dots - a_nx^n$.

— The ring $R[x]$ is also called the ring of polynomials over R and the elements of $R[x]$ are called polynomials over R.

— It is easy to verify that

(i) If R is commutative then $R[x]$ is also commutative

(ii) If R has unity 1 then $R[x]$ also has unity where $1 = 1 + 0x + 0x^2 + \dots\dots$

(iii) If F is a field then $F[x]$ is commutative ring with unity. However $F[x]$ is not a field.

EX: $f(x) = 1\cdot x \in F[x]$ (i.e, $f(x) = \overset{0}{\overset{\shortparallel}{a_0}} + a_1 x$) has no multiplicative inverse in $F[x]$.

Since if $g(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m \in F[x]$ the multiplicative inverse of $f(x)$ then $f(x) g(x) = 1$.

i.e, $c_0 + c_1 x + c_2 x^2 + \dots = 1 + 0x + 0x^2 + \dots$

$\Rightarrow c_0 = 1, c_1 = 0, c_2 = 0, \dots$

$\Rightarrow a_0 b_0 = 1$

$\Rightarrow 0 \cdot b_0 = 1$

$\Rightarrow 0 = 1$

which is a contradiction.

→ If R is an ID then $R[x]$ is an Integral Domain.

Soln: Since R is commutative

$\Rightarrow R[x]$ is commutative ring.

Now $R[x]$ has no zero divisors.

Let $f(x) \neq 0$, $g(x) \neq 0 \in R[x]$

where $f(x) = a_0 + a_1 x + \dots + a_n x^n$

$g(x) = b_0 + b_1 x + \dots + b_m x^m$.

$a_n \neq 0$, $b_m \neq 0 \in R$.

Then $f(x) \cdot g(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n+m} x^{n+m}$

where $c_{n+m} = a_n b_m \neq 0$

(Since R is an I.D)

$\therefore f(x) g(x) \neq 0 \in R[x]$

$\therefore R[x]$ is an Integral Domain.

→ If F is a field then $F[x]$ is an ID.

Sol^n: Since F is a field.

$\Rightarrow F$ is an ID

$\therefore F[x]$ is an ID.

Degree of a polynomials

Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$

we say that $f(x)$ is a non-zero polynomial, if atleast one of the coefficients $a_0, a_1, a_2, \ldots$ is not zero.

we say that $f(x)$ has degree 'n' if $a_n \neq 0$.

we write it as $\deg(f(x)) = n$

(or) $\deg f = n$

i.e, the highest power of x in the polynomial is called its degree

Note: (1) The degree of polynomial non-negative.

(2) The degree of zero polynomial is undefined.

i.e, the polynomial $0x^0 + 0x^1 + 0x^2 + \cdots$ has no degree

(3) The degree of a constant polynomial is zero.

i.e, the polynomial a_0x^0 $(a_0 \neq 0)$ has degree zero.

Ex:

→ Let $f(x) = 2+3x+5x^2$ and $g(x) = 3-5x+x^3$ be two polynomials over the ring of integers.

$\deg f = 2$, $\deg g = 3$.

we have $f(x)+g(x) = 5-2x+5x^2+x^3$ and

$f(x)\,g(x) = 6 - x - 23x^3 + 3x^4 + 5x^5.$

$\therefore \deg(f+g) = 3$ and $\deg(fg) = 5.$

→ Let $f(x)$ and $g(x)$ be two non-zero polynomials in $R[x]$ of degree m and n respectively, R being any ring.

Then (i) $\deg(f(x)+g(x)) = \operatorname{Max}(m,n)$ when $m \neq n$

(ii) $\deg(f(x)+g(x)) \leq m$ – when $m=n$

provided $f(x)+g(x)$ is not a zero polynomial.

Ex-①: Let $f(x) = 1+x+x^2$ and $g(x) = 2+3x+x^2$ be two polynomials over the ring of integers.

$\deg f = 2$, $\deg g = 2$

and $\deg(f+g) = 2$

$\deg(f+g) = 2 = \deg f$ (or) $\deg g$

Ex-②: Let $f(x) = 1+x+x^2$, $g(x) = 2+3x-x^2$.

then $f+g = 3+4x$

Now $\deg(f+g) = 1$.

$\therefore \deg(f+g) = 1 \leq \deg f$ (or) $\deg g$

→ If $f(x)$ & $g(x)$ are two non-zero polynomial elements of $F[x]$ and if $f(x)\cdot g(x) \neq 0$.

then $\deg(f(x)\cdot g(x)) \leq \deg f(x) + \deg g(x)$.

Ex:

Let $Z_4[x]$ be the ring of polynomials over the ring Z_4 of integers where $Z_4 = \{0, \bar{1}, 2, 3\}$

(i) Let $f(x) = x^2 + 2x + 3$ and $g(x) = 3x^2 + 2x$

then $f(x) + g(x) = (1+3)x^2 + (2+2)x + (3+0)$
$= 0x^2 + 0x + 3 = 3.$

$(\because 2+2 \equiv 0 \pmod 4$
$1+3 \equiv 0 \pmod 4)$

and $f(x) \cdot g(x) = (1 \cdot 3)x^4 + (1 \cdot 2 + 2 \cdot 3)x^3 + (2 \cdot 2 + 3 \cdot 3)x^2 + 2x$
$= 3x^4 + x^2 + 2x$

Now $\deg f = 2$, $\deg g = 2$
$\deg(f+g) = 0$ and $\deg(fg) = 4$
$\therefore \deg(f+g) \leq \text{Max}(2,2)$
and $\deg(fg) = 4 = \deg f + \deg g.$

(ii) Let $f(x) = 2x^2 + 2x + 3$ & $g(x) = 2x^2 + 2x$.

then $f(x) + g(x) = (2+2)x^2 + (2+2)x + 3$
$= 0x^2 + 0x + 3$
$= 3$

and $f(x) \cdot g(x) = (2 \cdot 2)x^4 + (2 \cdot 2)x^3 + (2 \cdot 2)x^3 + (2 \cdot 2)x^2$
$(3 \cdot 2)x^2 + (3 \cdot 2)x$
$= 0x^4 + 0x^3 + 0x^3 + 0x^2 + 2x^2 + 2x$
$= 2x^2 + 2x$

Now $\deg f = 2$, $\deg g = 2$
$\deg(f+g) = 0$ and $\deg(f \cdot g) = 2$
$\therefore \deg(f+g) \leq \text{Max}(2,2).$
and $\deg(f \cdot g) = 2 \leq \deg f + \deg g.$

→ If R is an ID then $\deg(fg) = \deg f + \deg g$

→ If R is an ID then $\deg f \leq \deg(fg)$

→ If $f(x), g(x)$ are two non-zero polynomials of $F[x]$ where F is a field then $\deg(fg) = \deg f + \deg g.$

→ Let $f(x)$ and $g(x)$ be two non-zero polynomials in $R[x]$, R being any ring.

(i) If $f(x)+g(x) \neq 0$ then $\deg(f(x)+g(x)) \leq \text{Max}(\deg f(x), \deg g(x))$

(ii) If $f(x)\cdot g(x) \neq 0$, then $\deg(f(x)\cdot g(x)) \leq \deg f(x) + \deg g(x)$.

(iii) If R is an integral domain, then
$$\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x).$$

Sol. Let $R[x]$ be the ring of polynomials of a ring R. Let $f(x)$ and $g(x)$ be two non-zero poly in $R[x]$ s.t. $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m \in R[x]$; $a_m \neq 0$
and $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_n x^n \in R[x]$; $b_n \neq 0$ in R.

Then we have $\deg f(x) = m$ & $\deg g(x) = n$.

Further $a_i = 0$ for $i > m$ and $b_j = 0$ for $j > n$.

(i) we have $f(x)+g(x) = (a_0+b_0)+(a_1+b_1)x+(a_2+b_2)x^2 + \cdots + (a_t+b_t)x^t$

where $t = \max(m,n)$.

Now $a_k + b_k = 0 \;\forall\; k > t$ as $a_k = 0, b_k = 0$.

$\therefore \deg(f(x)+g(x)) \leq t \;(= \max(m,n))$.

Note: it is possible to have $\deg(f(x)+g(x)) < \max(m,n)$

For example: Let us consider the ring Z of integers.

Let $f(x) = 1+2x-2x^2$
$g(x) = 2+3x+2x^2$ be two poly. in $Z[x]$.

then $f(x)+g(x) = 3+5x$.

$\therefore \deg(f(x) - g(x)) = 1$ where as
$\deg(f(x)) = 2 = \deg(g(x))$.

(ii) Let $f(x)\cdot g(x) = a_0b_0 + (a_0b_1 + a_1b_1 + a_2b_0)x + \cdots$
$\cdots\cdots + (a_0b_i + a_1b_{i-1} + a_2b_{i-2} + \cdots a_ib_0)x^i +$
$\cdots\cdots\cdots$

$= c_0 + c_1x + c_2x^2 + \cdots + c_ix^i + \cdots$

where $c_i = a_0b_i + a_1b_{i-1} + \cdots + a_ib_0$.

Here $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_mb_n$
$\cdots\cdots + a_{m+n}b_0$.

$= a_mb_n$ as all other terms are equal to zero.
(i.e $a_{m+i} = 0, b_{n+j} = 0$ for all $i, j > 0$)

Again $c_{m+n+t} = 0 \;\forall\, t > 0$.

Thus $\deg(f(x)\cdot g(x)) \le m+n$ ($a_mb_n = 0$ even if $a_m \neq 0, b_n \neq 0$)

Note(i): It is possible to have
$\deg(f(x)\cdot g(x)) < m+n$.

for example:
Let us consider the ring $Z_6 = \{0,1,2,3,4,5\}$ of integers under modulo 6.

Let $f(x) = 1 + 2x^3$
$g(x) = 2 + x + 3x^2$ be two elts in $Z_6[x]$.
of degree 3 and 2 respectively.

Here $f(x)\cdot g(x) = 2 + x + 3x^2 + 4x^3 + 2x^4$.
Clearly which is of degree $4 < 5$. (ie $3+2=5$)

Note(2) Here R is not ID.

Problems:

→ Find the sum and product of $f(x) = 5+4x+2x^2+2x^3$ and $g(x) = 1+4x+5x+x^3$ over $(\mathbb{Z}_6, +_6, \times_6)$.

→ $f(x) = \bar{1}+\bar{2}x$ and $g(x) = \bar{5}+\bar{4}x+\bar{3}x^2$ over $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Prove that $\deg(f(x) \cdot g(x)) \neq \deg f(x) + \deg g(x)$

Sol^n: $\deg f(x) = 1$; $\deg g(x) = 2$

$\Rightarrow \deg f(x) + \deg g(x) = 1+2 = 3$

Now $f(x) \cdot g(x) = (\bar{1}\times\bar{5}) + (\bar{1}\times\bar{4} + \bar{2}\times\bar{5})x + (\bar{1}\times\bar{3} + \bar{2}\times\bar{4})x^2 + (\bar{2}\times\bar{3})x^3$

$= \bar{5} + \overline{14}x + \overline{11}x^2 + \bar{6}x^3$

$= \bar{5} + \bar{2}x + \bar{5}x^2 + \bar{0}x^3$

$= \bar{5} + \bar{2}x + \bar{5}x^2$

$\therefore \deg(f(x) \cdot g(x)) = 2$

$\therefore \deg f(x) \cdot g(x) \neq \deg f(x) + \deg g(x)$.

→ Find the sum and product of the following polynomials

(i) $f(x) = 4x-5$, $g(x) = 2x^2-4x+2$ in $\mathbb{Z}_8[x]$

(ii) $f(x) = 1+3x$, $g(x) = 4+5x+2x^3$ in $\mathbb{Z}_7[x]$

(iii) $f(x) = 7+9x+5x^2+11x^3-2x^4$, $g(x) = 3-2x+7x^2+8x^3$ over the ring of integers

(iv) $f(x) = 2x^3+4x^2+3x+2$, $g(x) = 3x^4+2x+4$ over the ring $\mathbb{Z}_5 = \{0,1,2,3,4\}$ of mod 5.

(v) $f(x) = 4x^3+2x^2+x+3$, $g(x) = 3x^4+3x^3+3x^2+x+4$ in $\mathbb{Z}_5[x]$.

→ Over the ring $\mathbb{Z}_7 = \{0,1,2,3,4,5,6\}$ modulo 7, If $f(x) = 7+9x+5x^2+11x^3-2x^4$, $g(x) = 3-2x+7x^2+8x^3$.

P.T. $\deg(f(x)+g(x)) = 4$ and $\deg(f(x) \cdot g(x)) = 4$.

→ Let $f(x) = 2x^4 + 3x^3 + 2$ and $g(x) = 3x^5 + 4x^3 + 2x + 3$ be two polynomials over the field $Z_5 = (\{0,1,2,3,4\}, +_5, \times_5)$ Determine (i) $\frac{d}{dx} f(x)$ (ii) $f(x) \cdot g(x)$

→ If $f(x) = 3x^7 + 2x + 3$, $g(x) = 5x^3 + 2x + 6$ be two polynomials over the field $Z_7 = (\{0,1,2,3,4,5,6\}, +_7, \times_7)$ - Determine (i) $\frac{d}{dx} f(x)$ (ii) $f(x) \cdot g(x)$ (iii) $f(x) \pm g(x)$.

→ If R is an integral domain with unity, then the units of R and $R[x]$ are same.

Sol^n: Let a_0 be a unit of R. Then a_0 divides 1

i.e, $a_0 / 1$

i.e, there exists some $b_0 \in R$ such that

$a_0 b_0 = 1$.

Let $f(x) = a_0 + 0x + 0x^2 + \cdots$

$g(x) = b_0 + 0x + 0x^2 + \cdots$

Then $f(x), g(x) \in R[x]$. and

$f(x)\, g(x) = a_0 b_0 + 0x + 0x^2 + \cdots$

(or) $f(x)\, g(x) = 1$ $\quad (\because a_0 b_0 = 1)$

$\Rightarrow f(x)/1$ (i.e, $f(x)$ divides 1) in $R[x]$

$\Rightarrow f(x)$ is a unit in $R[x]$.

Hence $a_0 = f(x)$ is a unit in $R[x]$.

Conversely, let $f(x)$ be a unit of $R[x]$.

Then there exists some $g(x) \in R[x]$ such that

$f(x)\, g(x) = 1 = 1 + 0x + 0x^2 + \cdots$ ——— (1)

$\Rightarrow \deg(f(x)\, g(x)) = \deg(1 + 0x + 0x^2 + \cdots) = 0$

$\Rightarrow \deg f(x) + \deg g(x) = 0$ $\quad (\because R$ is I.D. $\deg(f(x)\, g(x)) = \deg f(x) + \deg g(x))$

$\Rightarrow \deg f(x) = 0$ and $\deg g(x) = 0$

$\Rightarrow f(x)$ and $g(x)$ are constant polynomials,

say $f(x) = \alpha$ $(\alpha \neq 0 \in R)$, $g(x) = \beta$ $(\beta \neq 0 \in R)$

$\Rightarrow \alpha\beta = 1$ by (1)

$\Rightarrow \alpha / 1$ (i.e, α divides 1) in R

Hence $f(x) = \alpha$ is a unit of R.

 (15)

(iii) If R is an ID then as $a_m \neq 0$, $b_n \neq 0$

therefore, $a_m \cdot b_n \neq 0$

$\Rightarrow C_{m+n} = a_m b_n \neq 0$

This shows that

$\deg(f(x)\,g(x)) = m+n.$

→ If $f(x), g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then

$$\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x).$$

Sol^n: Since every field is an integral domain, the result follows by above part (iii).

→ If $f(x), g(x)$ are two non-zero polynomials in $F[x]$ (F being a field), then

(i) $\deg f(x) \leq \deg(f(x)\,g(x))$

(ii) $\deg g(x) \leq \deg(f(x)\,g(x))$

Sol: we have

$$\deg(f(x)\,g(x)) = \deg f(x) + \deg g(x)$$
$$\geq \deg f(x), \text{ since } \deg g(x) \geq 0$$

$\therefore \deg f(x) \leq \deg(f(x)\,g(x))$

Similarly, $\deg g(x) \leq \deg(f(x)\,g(x))$

In order for $F[x]$ to be a Euclidean ring with the degree function acting as the d-function of Euclidean ring we still need that given $f(x), g(x) \in F[x]$, there exist $t(x), r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This is provided us by

LEMMA (THE DIVISION ALGORITHM) :-

Let $f(x)$ and $g(x)$ be two non-zero polynomials in $F[x]$ (F being a field), then $\exists$ unique polynomials $t(x)$ and $r(x)$ in $F[x]$ such that $f(x) = t(x)g(x) + r(x)$ where $r(x)$ or $\deg r(x) < \deg g(x)$.

Sol Let us consider the set

$S = \{ f(x) - h(x)g(x) \,/\, h(x) \in F[x] \}$.

for $0(x) \in F[x]$,

$f(x) = f(x) - 0(x).g(x) \in S$.

$\therefore S \neq \phi$.

Let $0 \in S$. Then by definition of S, $\exists\, q(x) \in F[x]$ so that $0 = f(x) - q(x)g(x)$

i.e $f(x) = q(x)g(x) + 0(x)$

i.e $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$.

$\therefore$ the theorem is proved.

Let $0(x) \notin S$. Then every polynomial in S is a non-zero polynomials and hence non-negative degree.

Let $r(x) \in S$ be a polynomial of least degree.

By definition of S, there exist $q(x) \in F[x]$ so that

$r(x) = f(x) - q(x)g(x)$

i.e $f(x) = g(x)q(x) + r(x)$. —(1)

Let $g(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_n \neq 0$

So that $\deg g(x) = n$

NOW we have to prove that $\deg r(x) < n$.

i.e $\deg r(x) < \deg g(x)$.

If possible, suppose that $m = \deg r(x) \geq n$.

Let $r(x) = c_0 + c_1x + c_2x^2 + \cdots + c_mx^m$, $c_m \neq 0$.

NOW we have

$$c_m a_n^{-1} x^{m-n} g(x) = c_m a_n^{-1} x^{m-n} [a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n]$$

$$= c_m a_n^{-1} a_0 x^{m-n} + c_m a_n^{-1} a_1 x^{m-n+1} + \cdots + c_m a_n^{-1} a_{n-1} x^{m-1} + c_m x^m.$$

$\therefore r(x) = c_m a_n^{-1} x^{m-n} g(x)$

$= (c_{m-1}x^{m-1} + \cdots + c_0) -$

$(c_m a_n^{-1} a_{n-1} x^{m-1} + \cdots + c_m a_n^{-1} a_0 x^{m-n})$

$\therefore r(x) = c_m a_n^{-1} x^{m-n} g(x) + \alpha(x)$ — (2)

where $\alpha(x) = (c_{m-1} - c_m a_n^{-1} a_{n-1}) x^{m-1} + \cdots + c_0$

$\Rightarrow \deg \alpha(x) \leq m-1$.

i.e $\deg \alpha(x) \leq \deg r(x) - 1$

i.e $\deg \alpha(x) < \deg r(x)$.

$\therefore$ From (1) & (2);

$\alpha(x) = f(x) - g(x) \{q(x) + c_m a_n^{-1} x^{m-n}\}$.

$= f(x) - g(x) \beta(x)$,

where $\beta(x) = q(x) + c_m a_n^{-1} x^{m-n} \in F[x]$.

$\therefore \alpha(x) \in S$.

NOW we have, $\alpha(x), r(x) \in S$ and $\deg \alpha(x) < \deg r(x)$.

This is a contradiction. Since $r(x)$ is the polynomial of least degree in S.

$\therefore$ Our supposition is wrong.

Hence $\deg r(x) < n$

i.e $\deg r(x) < \deg g(x)$.

$\therefore \exists\, q(x), r(x) \in F[x]$ so that

$f(x) = q(x)\,g(x) + r(x)$ where $r(x) = 0(x)$ (or) $\deg r(x) < \deg g(x)$.

Uniqueness of $q(x)$ and $r(x)$:-

If possible, suppose that $f(x) = q'(x)g(x) + r'(x)$

where $r'(x) = 0$ or $\deg r'(x) < \deg g(x)$.

Then $q(x)g(x) + r(x) = q'(x)g(x) + r'(x)$

i.e $(q(x) - q'(x))g(x) = r'(x) - r(x)$

If $q(x) - q'(x) \neq 0$ then $\deg(q(x) - q'(x))g(x) = \deg(q(x) - q'(x)) + \deg g(x)$.

i.e $\deg(r'(x) - r(x)) \geq \deg g(x)$.

This is a contradiction because $\deg r(x) < \deg g(x)$ and $\deg r'(x) < \deg g(x)$.

$\therefore q(x) - q'(x) = 0$ and $r'(x) - r(x) = 0$

$\Rightarrow q'(x) = q(x)$ & $r'(x) = r(x)$.

Hence $q(x), r(x) \in F[x]$ are unique.

Note: (1). The polynomials $q(x)$ and $r(x)$ of the above theorem are called the quotient and the remainder.

(2). In the above theorem if $r(x)=0$ then we say that $q(x)$ divides $f(x)$ or $g(x)$ is a factor of $f(x)$.

→ If F is a field, then $F[x]$ is a Euclidean domain.

Soln: Let F be a field

Then F is an ID

$\therefore$ $F[x]$ is an ID.

Further for any two non-zero polynomials $f(x)$ and $g(x)$ in $R[x]$,

we have $\deg(f(x)\cdot g(x)) = \deg f(x) + \deg g(x)$
$\geq \deg f(x)$

$(\because \deg g(x) \geq 0)$.

$\therefore \deg f(x) \leq \deg(f(x)\, g(x))$ — (1)

Now we define the Euclidean valuation d on $F[x]$ as follows:

$d(f) = d(f(x)) = \deg f(x)$ $\forall$ $f(x) \neq 0$ in $F[x]$.

Then $d(f)$ is a non-negative integer, since $\deg f(x)$ is so. — (2)

From (1) and (2), we see that

$\deg(f) \leq \deg(fg)$ $\forall$ $f \neq 0, g \neq 0$ in $F[x]$

$\therefore$ By Division algorithm,

for $f(x) \neq 0$, $g(x) \neq 0$ in $F[x]$, $\exists$ $t(x)$, $r(x)$ in $F[x]$

such that $f(x) = t(x)\,g(x) + r(x)$, where

$r(x) = 0$ or $\deg r(x) < \deg g(x)$

$\therefore$ $f = tg + r$, where $r=0$ or $d(r) < d(g)$.

Hence $F[x]$ is a Euclidean domain.

→ If F is a field, $F[x]$ is a principal ideal domain.

Sol^n: Let U be an ideal of $F[x]$ and $U = \{0\}$ where 0 is the zero polynomials.

Then $U = \langle 0 \rangle$, the principal ideal generated by 0.

Let U be an ideal of $F[x]$ and $U \neq \{0\}$.

Then U contains polynomials of non-negative degree.

By well ordering principle $\exists$ a polynomial $f(x) \in U$, $f(x) \neq 0$ such that $\deg f(x) \leq \deg g(x)$ where $g(x)$ is any polynomial in U and $g(x) \neq f(x)$.

Let $h(x)$ be any polynomial in U.

By the division algorithm, $\exists$ polynomials $q(x), r(x)$ in $F[x]$ such that

$h(x) = f(x)\, q(x) + r(x)$ where $r(x) = 0$ or $\deg r(x) < \deg f(x)$.

$f(x) \in U$, $q(x) \in F[x]$, U is an ideal $\Rightarrow f(x)\, q(x) \in U$

$h(x) \in U$; $f(x)\, q(x) \in U \Rightarrow h(x) - f(x)\, q(x) = r(x) \in U$

Now $r(x) \in U$, $r(x) = 0$ or $\deg r(x) < \deg f(x)$

$\Rightarrow r(x) = 0$

$\therefore h(x) = f(x)\, q(x)$ where $q(x) \in F[x]$.

$\therefore U = \{ f(x)\, q(x) / q(x) \in F[x] \} = \langle f(x) \rangle$ is the principal ideal generated by $f(x)$.

Hence every ideal U of $F[x]$ is a principal ideal.

→ $Z[x]$ over the ring of integers is not a principal ideal ring.

01:

Let $S = \{x, 2\} \subset Z[x]$ be a subset containing two elements.

we show that ideal generated by $S = (x, 2)$ is not a principal ideal of $Z[x]$.

If possible, let $(x,2)$ be a principal ideal of $Z[x]$

$\therefore \exists\ a(x) \in Z[x]$ so that $(x,2) = [a(x)]$

$x \in [a(x)] \Rightarrow \exists\ b(x) \in Z[x]$ so that $x = a(x)\, b(x)$ — (1)

$2 \in [a(x)] \Rightarrow \exists\ c(x) \in Z[x]$ so that $2 = a(x)\, b(x)$ — (2)

$\therefore \deg [a(x)\ b(x)] = \deg x \Rightarrow \deg a(x) + \deg b(x) = 1$ — (3)

$\deg [a(x)\ c(x)] = \deg 2 \Rightarrow \deg a(x) + \deg c(x) = 0$ — (4)

From (4); $\deg a(x) = 0$ and $\deg c(x) = 0$.

$\Rightarrow a(x), c(x)$ are non-zero constant polynomials.

$\Rightarrow a(x), c(x)$ are non-zero integers.

Again, $a(x) \cdot c(x) = 2 \Rightarrow a(x), c(x)$ are non-zero integers with the following four alternatives.

$a(x) = 1\ ,\ c(x) = 2$

$a(x) = -1\ ,\ c(x) = -2$

$a(x) = 2;\ c(x) = 1$

$a(x) = -2,\ c(x) = -1$

If $a(x) = \pm 1$, we have $[a(x)] = Z[x]$

This is a contradiction to $[a(x)] = (x,2)$;

Again, if $a(x) = \pm 2$ then from (2)

$x = a(x)\ c(x) \Rightarrow x = \pm 2(c_0 + c_1 x + \cdots)$

$\Rightarrow 1 = \pm 2c_1$ where $c_1 \in Z$

This is also a contradiction as there exists no integers c_1 so that $1 = \pm 2c_1$.

$\therefore$ Our supposition that $(x,2)$ is a principal ideal is wrong.

Hence $Z[x]$ is not a principal ideal ring.

Then by uniqueness of the factorization, we have $a \sim b_i$ for some i or $a \sim c_j$ for some j. If $a \sim b_i$, then $a \mid b_i$ and hence $a \mid b$. On the other hand, if $a \sim c_j$, then $a \mid c_j$, which implies that $a \mid c$. Thus $a \mid b$ or $a \mid c$. Hence a is prime. □

Corollary 13.1.16. *Let R be a UFD and p be a nonzero nonunit element of R. Then p is irreducible if and only if p is prime.*

Proof. Follows from the above theorem and Theorem 13.1.6(iii). □

Theorem 13.1.17. *A factorization domain R is a UFD if and only if every irreducible element of R is prime.*

Proof. One side follows from Theorem 13.1.15. Let R be a factorization domain in which every irreducible element is prime. We show that R is a UFD. Since R is a FD, it is sufficient to show that factorization of a nonzero nonunit element a of R in terms of irreducible (hence prime) elements is unique.

Now to show the uniqueness of the representation of a as a product of primes, we assume that a can be expressed as a product of primes in two ways, say,

$$a = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_r, \tag{13.1.2}$$

where p_i and q_j are primes. Suppose $t > r$. Now $p_1 \mid a$. Hence $p_1 \mid q_1 q_2 \cdots q_r$. Then by Problem 9 of Exercises 13.1, p_1 divides one of $q_1, q_2, \ldots, q_r$. By relabelling, if necessary, we may assume $p_1 \mid q_1$. Since q_1 is irreducible, p_1 is an associate of q_1. Hence $q_1 = p_1 u_1$ for some unit $u_1 \in R$. Thus,

$$p_1 p_2 \cdots p_t = p_1 u_1 q_2 \cdots q_r \qquad (*)$$

and by cancellation (since R is a domain), $p_2 p_3 \cdots p_t = u_1 q_2 \cdots q_r$.

Again $p_2 \mid u_1 q_2 \cdots q_r$. Since u_1 is a unit, $p_2 \nmid u_1$. Hence p_2 divides one of $q_2, q_3, \ldots, q_r$. Assume as above, $p_2 \mid q_2$. Then $q_2 = p_2 u_2$ where u_2 is a unit and

$$p_2 p_3 \cdots p_t = p_2 u_2 u_1 q_3 \cdots q_r.$$

Again by cancellation,

$$p_3 p_4 \cdots p_t = u_1 u_2 q_3 \cdots q_r.$$

Repeating this process we obtain,

$$p_{r+1} p_{r+2} \cdots p_t = u_1 u_2 \cdots u_r.$$

 3

This implies that p_{r+1} divides a unit, which is a contradiction. Hence $t \not> r$. Similarly, we can show that $r \not> t$. Consequently, $r = t$ and also we find that p_i and q_i are associates for $i = 1, 2, \ldots, r$. This proves the uniqueness. □

Let us now consider the domain $\mathbb{Z}[\sqrt{-5}]$ once again. We have shown that it is a FD. In this domain, 3 is irreducible but not a prime element. Hence from Theorem 13.1.17, it follows that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Thus we see that, like PID, in the case of UFD also, there is no difference between prime and irreducible elements. In fact, we show that any PID is a UFD. We proceed through some preliminary lemmas.

Lemma 13.1.18. *Let R be a PID. If (a_n), $n \in \mathbb{N}$ be any infinite sequence of principal ideals of R such that*

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots,$$

then there exists $m \in \mathbb{N}$ so that $(a_n) = (a_m)$ for all $n \geq m$.

Proof. We have $I = \bigcup_{n \in \mathbb{N}} (a_n)$ is an ideal of R. Now since R is a PID, $I = (a)$ for some $a \in R$. Since $a \in I$, $a \in (a_m)$ for some $m \in \mathbb{N}$. Therefore, $I = (a) \subseteq (a_m) \subseteq (a_n) \subseteq I$ for all $n \geq m$. This implies $(a_n) = (a_m)$ for all $n \geq m$. □

Lemma 13.1.19. *Let a be a nonzero nonunit element of a PID R. Then there exists a prime element $p \in R$ such that $p \mid a$.*

Proof. Since a is not a unit, we have $(a) \neq R$. Observe that either (a) is itself a maximal ideal of R or else there exists $a_1 \in R$ such that $(a) \subset (a_1)$. If (a_1) is a maximal ideal, then call it M. Otherwise, there exists $a_2 \in R$ such that $(a_1) \subset (a_2)$. Proceeding in this way, we get a strictly ascending chain of principal ideals in the PID R. Then by the above lemma, this chain must terminate after finite steps and we find a maximal ideal M of R such that $(a) \subseteq M$. Now since R is a PID, $M = (p)$ for some prime $p \in R$, by Theorem 13.1.9. Then $(a) \subseteq (p)$ which implies that $p \mid a$, as required. □

Lemma 13.1.20. *If R is a PID, then every nonzero nonunit element of R has a factorization into a finite product of prime elements.*

Proof. Let a be a nonzero nonunit element of R. By Lemma 13.1.19, there exists a prime element p_1 in R such that $p_1 \mid a$. Then $a = p_1 a_1$ for some $0 \neq a_1 \in R$. Thus $(a) \subseteq (a_1)$. If $(a) = (a_1)$, then we have $a_1 = ra$ for some $r \in R$. Then $a = p_1 a_1 = p_1 r a$ which implies that $p_1 r = 1$, as R is an integral domain. But then p_1 becomes a unit, which is a contradiction. Therefore $(a) \subset (a_1)$. If $(a_1) \neq R$, then a_1 is not a unit. Also $a_1 \neq 0$. So we can repeat the process on a_1, whereby we get an increasing chain of principal ideals:

$$(a) \subset (a_1) \subset (a_2) \subset \cdots \subset (a_n) \subset \cdots$$

with $a_{i-1} = p_i a_i$ for some prime $p_i \in R$. We continue the process until a_n becomes a unit for some n. The sequence must terminate because of Lemma 13.1.18. Therefore,

$$(a) \subset (a_1) \subset \cdots \subset (a_n) = R,$$

as a_n is a unit. So we have

$$a = p_1 a_1 = p_1 p_2 a_2 \cdots = p_1 p_2 \cdots p_{n-1} a_{n-1},$$

where $a_{n-1} = p_n a_n$. Now since p_n is a prime and a_n is a unit, a_{n-1} is an associate of prime and so it is itself a prime. This completes the proof. □

Theorem 13.1.21. *Every PID is a UFD.*

Proof. By Lemma 13.1.20, each nonzero nonunit element has a factorization. Hence it follows that every PID is a FD. Again in a PID, every irreducible element is a prime element. Hence from Theorem 13.1.17, it follows that every PID is a UFD. □

Interestingly, the converse of the above theorem is not true. Indeed, we have already mentioned that $\mathbb{Z}[x]$ is a UFD but later on we shall prove that $\mathbb{Z}[x]$ is not a PID (cf. Worked Out Exercise 13.1.5).

Worked Out Exercises

◊ **Exercise 13.1.1.** Determine all the associates of $1 + i\sqrt{5}$ in $\mathbb{Z}[i\sqrt{5}]$.

Solution. We know that the only units of $\mathbb{Z}[i\sqrt{5}]$ are 1 and -1. This implies that the associates of $1 + i\sqrt{5}$ are $1 + i\sqrt{5}$ itself and $-1 - i\sqrt{5}$.

◊ **Exercise 13.1.2.** Find a prime element in $\mathbb{Z}_{10}$ which is not irreducible.

Solution. Consider the element $[2] \in \mathbb{Z}_{10}$. We show that $[2]$ is prime but not irreducible. Let $[a], [b] \in \mathbb{Z}_{10}$ be such that $[2] \mid [a][b]$. Then we have $2k \equiv ab \pmod{10}$ for some integer k which implies that $ab = 2k + 10n$ for some integer n. Therefore ab is even and so at least one of a and b is even which proves that $[2]$ divides $[a]$ or $[b]$. Hence $[2]$ is prime in $\mathbb{Z}_{10}$.

The prime element $[2]$ is not irreducible as $[2] = [32] = [4][8]$ but none of $[4]$ and $[8]$ are units in $\mathbb{Z}_{10}$.[1]

◊ **Exercise 13.1.3.** Show that the integral domain $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ is a FD.

Solution. Define $\delta : \mathbb{Z}[\sqrt{3}] \setminus \{0\} \to \mathbb{N}$ as follows: for all $a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, $\delta(a + b\sqrt{3}) = |a^2 - 3b^2|$. Now $\delta(a + b\sqrt{3}) = 1$ if and only if $|a^2 - 3b^2| = 1$ if and only if $(a + b\sqrt{3})(a - b\sqrt{3}) = \pm 1$ if and only if $a + b\sqrt{3}$ is a unit. Let $a + b\sqrt{3}, c + d\sqrt{3}$ be two nonzero elements of $\mathbb{Z}[\sqrt{3}]$. Then $\delta((a + b\sqrt{3})(c + d\sqrt{3})) = |a^2 - 3b^2||c^2 - 3d^2| \geq |c^2 - 3d^2| = \delta(c + d\sqrt{3})$, where equality holds if and only if $\delta(a + b\sqrt{3}) = 1$, i.e., if and only if $a + b\sqrt{3}$ is a unit. Hence $\mathbb{Z}[\sqrt{3}]$ is a FD.

◊ **Exercise 13.1.4.** Let N_1 be the set of all natural numbers greater than 1. Call an integer $n \in N_1$ *square free* if n is not divisible by the square of any integer that belongs to N_1. Consider the domain $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ for some square free integer $n \in N_1$. Prove that $a + b\sqrt{n}$ is irreducible in $\mathbb{Z}[\sqrt{n}]$ if $|a^2 - nb^2|$ is prime in $\mathbb{Z}$.

Solution. Let $a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ be such that $|a^2 - nb^2|$ is a prime number, say p. Now if $a + b\sqrt{n} = (c + d\sqrt{n})(e + f\sqrt{n})$, then $a = ce + ndf$ and $b = cf + de$. Thus $p = |a^2 - nb^2| = |(ce + ndf)^2 - n(cf + de)^2| = |c^2e^2 + 2ncdef + n^2d^2f^2 - n(c^2f^2 + 2cdef + d^2e^2| = |(c^2 - nd^2)(e^2 - nf^2)| = |c^2 - nd^2||e^2 - nf^2|$. Since p is prime, we have either $|c^2 - nd^2| = 1$ or $|e^2 - nf^2| = 1$. If $|c^2 - nd^2| = 1$, then we have $|(c + d\sqrt{n})(c - d\sqrt{n})| = 1$ which implies $c + d\sqrt{n}$ is a unit in $\mathbb{Z}[\sqrt{n}]$ with $(c + d\sqrt{n})^{-1} = c - d\sqrt{n}$ or $-(c - d\sqrt{n})$. Similarly if $|e^2 - nf^2| = 1$, then we have that $e + f\sqrt{n}$ is a unit in $\mathbb{Z}[\sqrt{n}]$. Thus $a + b\sqrt{n}$ is irreducible in $\mathbb{Z}[\sqrt{n}]$.

◊ **Exercise 13.1.5.** Find an ideal in the polynomial ring $\mathbb{Z}[x]$ which is not a principal ideal. Hence justify that $\mathbb{Z}[x]$ is not a PID.

[1] Recall that $[r]$ is a unit in $\mathbb{Z}_n$ if and only if $\gcd(n, r) = 1$.

Let us now exploit another nice property of the ring of integers. Let $n > 1$ be a positive integer. Then n can be expressed uniquely as a product of prime numbers. Since $\mathbb{Z}$ is a PID, prime numbers and irreducible elements of $\mathbb{Z}$ are indistinguishable. We now define a class of integral domains in which every nonzero nonunit element can be factorized in terms of irreducible elements.

Definition 13.1.10. Let a be a nonzero nonunit element in an integral domain R. If $a = p_1p_2\ldots p_r$ where $p_1, p_2, \ldots, p_r$ are irreducible elements in R, then $p_1p_2\ldots p_r$ is called a *factorization* of a in R. An integral domain R is called a *factorization domain* (in short, *FD*), if every nonzero nonunit element in R has a factorization in terms of irreducible elements of R.

Clearly, the ring of integers is a FD. To give some other examples of FD, we prove the following theorem.

Theorem 13.1.11. *Let R be an integral domain. Suppose there exists a function $\delta : R \setminus \{0\} \to \mathbb{N}_0$ such that, for all $a, b \in R \setminus \{0\}$, $\delta(ab) \geq \delta(b)$, where equality holds if and only if a is a unit. Then R is a FD.*

Proof. Suppose R is not a FD. Hence there exists a nonzero nonunit element a such that a is not factorizable. Let $T = \{b \in R \mid b$ is a nonzero non-unit but not factorizable$\}$. Hence $T \neq \emptyset$. Let $T_1 = \{\delta(b) \mid b \in T\}$. Now T_1 is a nonempty subset of $\mathbb{N}_0$. Hence by the well-ordering principle, T_1 has a least element. So, we can find an element $b \in T$ such that $\delta(b) \leq \delta(a)$ for all $a \in T$. Since $b \in T$, b is a nonzero nonunit and also not irreducible. Note that, every irreducible element gives a factorization of itself. Hence there exist nonzero nonunit elements $c, d \in R$ such that $b = cd$. Now at least one of c, d does not have a factorization, otherwise, the factorizations of c and d put together produce a factorization of b. Suppose c is not factorizable. Then $c \in T$ and hence $\delta(c) \in T_1$. Since d is not a unit, we find that $\delta(b) > \delta(c)$. This contradicts the fact that $\delta(b)$ is the least element in T_1. Hence R is a FD. □

By virtue of this theorem, we can find different examples of factorizable domains.

Example 13.1.12. (i) $\mathbb{Z}$ is a FD, because we have a function $\delta(a) = |a|$ which satisfies the conditions of the above theorem.

(ii) $\mathbb{Z}[i]$ is a FD, since $\delta(a + ib) = a^2 + b^2$ is a function satisfying the given conditions.

(iii) Consider the domain $\mathbb{Z}[\sqrt{-5}]$. Define $\delta : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ by $\delta(a+b\sqrt{-5}) = a^2 + 5b^2$. We have already shown that $a + b\sqrt{-5}$ is a unit in $\mathbb{Z}[\sqrt{-5}]$ if and only if $a^2 + 5b^2 = 1$, i.e., if and only if $\delta(a + b\sqrt{-5}) = 1$. Let $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \setminus \{0\}$. Then,

$$\begin{aligned}
&\delta((a + b\sqrt{-5})(c + d\sqrt{-5}))\\
= {}&\delta((ac - 5bd) + (ad + bc)\sqrt{-5})\\
= {}&(ac - 5bd)^2 + 5(ad + bc)^2\\
= {}&(a^2 + 5b^2)(c^2 + 5d^2)\\
\geq {}&a^2 + 5b^2 \quad \text{(equality holds if and only if } c^2 + 5d^2 = 1).
\end{aligned}$$

Hence $\mathbb{Z}[\sqrt{-5}]$ is a FD.

Definition 13.1.13. An integral domain R is called a *unique factorization domain* (in short, *UFD*)[2], if the following conditions are satisfied:

(i) for every nonzero nonunit element $a \in R$, $a = a_1a_2\cdots a_n$ for some positive integer n, where each a_i is irreducible;

(ii) if $a = a_1a_2\cdots a_n = b_1b_2\cdots b_m$ where a_i and b_i are irreducible, then $m = n$ and each $a_i \sim b_{\sigma(i)}$ for some permutation σ on the set $\{1, 2, \ldots, n\}$.

Example 13.1.14. Certainly, $\mathbb{Z}$ is an example of a UFD. In the sequel we shall show that any PID is a UFD. Also the famous Gauss' theorem, that we shall discuss in the next chapter (cf. Theorem 14.1.27), will assure us that a polynomial ring over a UFD is again a UFD. In particular, $\mathbb{Z}[x]$ is a UFD.

Theorem 13.1.15. *Every irreducible element in a UFD is prime.*

Proof. Let $a \in R$ be irreducible and $a \mid bc$ for some $b, c \in R$. If either b or c is zero, then a divides one of b, c. So suppose $b \neq 0$, $c \neq 0$. If one of b or c is a unit, then $bc \sim c$ or $bc \sim b$ which implies that $a \mid c$ or $a \mid b$, i.e., a is prime. Hence, assume neither b nor c is a unit.

Now since $a \mid bc$, there exists $x \in R$ so that $ax = bc$. It follows that x must be a nonzero nonunit (prove it!) element. Since R is a UFD, we have the unique (up to associates) factorization in terms of irreducible elements on both sides of the above equality, namely,

$$au_1u_2\cdots u_r = b_1b_2\cdots b_s \cdot c_1c_2\cdots c_t \text{ (say)}.$$

[2] Also called *Gaussian domain*.

Conversely, suppose that $a^2+5b^2=1$. Then $(a+b\sqrt{-5})(a-b\sqrt{-5})=1$. Hence $(a+b\sqrt{-5})$ is a unit. Now if $a^2+5b^2=1$, then $a=\pm1$ and $b=0$ as $a,b\in\mathbb{Z}$. Hence it follows that 1 and -1 are the only units of $\mathbb{Z}[\sqrt{-5}]$.

(ii) $1+\sqrt{-5}$, $1-\sqrt{-5}$, 3, 2 are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$: We show that 3 is an irreducible element. Let $3=(a+b\sqrt{-5})(c+d\sqrt{-5})$, where $(a+b\sqrt{-5}),(c+d\sqrt{-5})\in\mathbb{Z}[\sqrt{-5}]$. Then proceeding as above, we have $3=(a-b\sqrt{-5})(c-d\sqrt{-5})$, whence

$$9=3\cdot3=(a^2+5b^2)(c^2+5d^2) \qquad (13.1.1)$$

Now there are no $a,b,c,d\in\mathbb{Z}$, for which $a^2+5b^2=3$ and $c^2+5d^2=3$. Hence (13.1.1) implies that either $a^2+5b^2=1$ or $c^2+5d^2=1$, i.e., either $a+b\sqrt{-5}$ is a unit or $c+d\sqrt{-5}$ is a unit. So, we see that 3 is an irreducible element in $\mathbb{Z}[\sqrt{-5}]$. Similarly, one can show that 2, $1+\sqrt{-5}$, $1-\sqrt{-5}$ are irreducible elements in $\mathbb{Z}[\sqrt{-5}]$.

(iii) $1+\sqrt{-5}$, $1-\sqrt{-5}$, 3, 2 are not prime elements in $\mathbb{Z}[\sqrt{-5}]$: We prove it for 3, and leave the rest of the similar verifications for the reader. Since $3\cdot2=6$, we find that $3\mid6$. But $6=(1+\sqrt{-5})(1-\sqrt{-5})$. Hence $3\mid(1+\sqrt{-5})(1-\sqrt{-5})$. Suppose $3\mid1+\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. Then there exists $u+v\sqrt{-5}\in\mathbb{Z}[\sqrt{-5}]$ such that $3(u+v\sqrt{-5})=1+\sqrt{-5}$. This implies that $3u=1$ and $3v=1$. But there are no integers u,v for which $3u=1$ or $3v=1$. Hence $3\nmid1+\sqrt{-5}$. Similarly, we can show that $3\nmid1-\sqrt{-5}$. Consequently, 3 is not a prime element.

In the part (iii) of Theorem 13.1.6, we have seen that in any integral domain, every prime element is irreducible. But we have shown in the domain $\mathbb{Z}[\sqrt{-5}]$ that 3 is an irreducible element which is not a prime. An interesting point to note is that, there are some special integral domains where the distinction between these two concepts disappears. Now we are going to consider one such class of integral domains.

Recall that an integral domain R is said to be a *principal ideal domain* (in short, *PID*), if every ideal of R is a principal ideal.

Example 13.1.7. (i) Consider the ring of integers, $\mathbb{Z}$. It is an integral domain. Also by Worked out Exercise 12.1.2, we know that every ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}=(n)$ for some nonnegative integer n. Thus $\mathbb{Z}$ is an example of PID.

(ii) In the next chapter, we shall see that the polynomial ring $\mathbb{R}[x]$ over the field of real numbers is a PID. But the polynomial ring $\mathbb{Z}[x]$ is not a PID.

Theorem 13.1.8. *In a PID R, a nonzero nonunit element p is irreducible if and only if p is prime.*

Proof. Let p be an irreducible element. Suppose $a,b\in R$ be such that $p\mid ab$. Then $ab=pv$ for some $v\in R$. Let $I=\{rb+tp\mid r,t\in R\}$. It can be easily shown that I is an ideal. Since R is a PID, there exists $d\in R$ such that $I=(d)$. Now $p=0b+1p\in(d)$. Hence $p=du$ for some $u\in R$. Since p is irreducible, either d is a unit or u is a unit. If d is unit, $1\in(d)=I$. Hence $1=rb+tp$ for some $r,t\in R$. Then $a=rab+tap=rpv+tap=p(rv+ta)$ implies that $p\mid a$.

If u is a unit, then $d=pu^{-1}\in(p)$. Thus $I=(d)\subseteq(p)\subseteq I$, so that $I=(p)$. Now $b=1b+0p\in I$. Hence $b\in(p)$, which implies that $p\mid b$. Thus we find that either $p\mid a$ or $p\mid b$. Hence p is a prime element.

The converse follows from part (iii) of Theorem 13.1.6. □

The following theorem describes the relation among maximal ideals, prime ideals, irreducible elements and prime elements in a PID.

Theorem 13.1.9. *Let p be an element of a PID R. Then the following are equivalent:*

(i) p is irreducible.
(ii) (p) is a nonzero maximal ideal.
(iii) (p) is a nonzero prime ideal.
(iv) p is prime.

Proof. (i) ⇒ (ii) Let p be an irreducible element in a PID R. Then by definition, p is nonzero and nonunit. Hence $(p)\neq R$ and also $(p)\neq(0)$. Let J be an ideal of R such that $(p)\subset J$. Since R is a PID, there exists $d\in R$ such that $J=(d)$. Then $(p)\subset(d)$. Now $p\in(d)$. Hence $p=du$ for some $u\in R$. Since p is irreducible, either d is a unit or u is a unit. If d is a unit, then $1\in(d)=J$ which implies that $J=R$. If u is a unit, then $d=pu^{-1}$ shows that $J=(d)\subseteq(p)$, which contradicts our assumption that $(p)\subset J$. Hence if $(p)\subset J$, then $J=R$. Consequently, (p) is a maximal ideal.

(ii) ⇒ (iii) Follows from Theorem 12.3.8.

(iii) ⇒ (iv) Follows from Theorem 13.1.6(ii).

(iv) ⇒ (i) Follows from Theorem 13.1.6(iii). □

(ii) $a \sim b \iff (a) = (b)$;

(iii) the binary relation $\sim$ on R is an equivalence relation;

(iv) u is a unit in $R \iff u \sim 1 \iff (u) = R$;

(v) If R is an integral domain, then $a \sim b$ if and only if $a = bu$ for some unit u in R.

Proof. The proof for other parts being obvious, we only prove (v).

Let R be an integral domain. If $a \sim b$, then $a \mid b$ and $b \mid a$. These imply $a = bu$ and $b = av$ for some $u, v \in R$. Then $a = bu = (av)u$ and so $a(1 - vu) = 0$. Since R is an integral domain and $a \neq 0$, we have $1 - vu = 0$. Thus $vu = 1$. Since R is commutative, we have $v = u^{-1}$, i.e., u is a unit.

Conversely, let $a = bu$ where u is a unit in R. Then by definition, $b \mid a$. Also since u is a unit, $b = au^{-1}$, which implies $a \mid b$. Therefore $a \sim b$. □

The concept of *prime numbers* is very much associated with divisibility of integers. In the following, we define analogous concepts in the case of an arbitrary commutative ring with identity.

Definition 13.1.3. Let R be a commutative ring with identity. Then a *nonzero nonunit element* $p \in R$ is called *irreducible* in R, if $p = ab$ for some $a, b \in R$ implies, either a is a unit in R or b is a unit in R. On the other hand, a *nonzero nonunit element* p is called *prime* in R, if $p \mid ab$ for some $a, b \in R$ implies, either $p \mid a$ or $p \mid b$.

Example 13.1.4. (i) In the ring $\mathbb{Z}$, any prime number is *prime* as well as *irreducible*.

(ii) In the ring $\mathbb{Z}_6$, $[2]$ is *prime* but *not irreducible*, as $[2] = [2] \cdot [4]$ but neither $[2]$ nor $[4]$ is a unit in $\mathbb{Z}_6$.

(iii) The field $\mathbb{Q}$ of all rational numbers has neither any irreducible element nor any prime element, as every nonzero element of $\mathbb{Q}$ is a unit. Indeed, such an assertion is true for any field.

Remark 13.1.5. Note that in an integral domain R, associates of an irreducible element of R are irreducible and associates of a prime element of R are prime (prove!).

Theorem 13.1.6. *Let p be a nonzero nonunit element in an integral domain R. Then*

(i) p is irreducible if and only if $d \mid p$, $d \in R$ implies that either d is a unit or $d \sim p$;[1]

(ii) p is prime if and only if (p) is a nonzero prime ideal of R;

(iii) If p is prime, then p is irreducible.

Proof. (i) Follows immediately from the definition of irreducible elements.

(ii) Suppose p is prime. Then $(p) \neq (0)$ as $p \neq 0$. Also since p is not a unit, (p) is a proper ideal of R. Now let $b, c \in R$ be such that $bc \in (p)$. Then $bc = px$ for some $x \in R$. So $p \mid bc$ which implies that $p \mid b$ or $p \mid c$, as p is prime. Therefore $b \in (p)$ or $c \in (p)$ and hence (p) is a prime ideal of R.

Conversely, let (p) be a nonzero prime ideal of R. Then $p \neq 0$ and since $(p) \neq R$, we find p is a nonunit element of R. Let $p \mid bc$ for some $b, c \in R$. Then $bc \in (p)$, which implies that $b \in (p)$ or $c \in (p)$, as (p) is a prime ideal of R. Thus $p \mid b$ or $p \mid c$, proving that p is prime.

(iii) Let p be a prime element of R and $p = bc$ for some $b, c \in R$. Since p is prime, we have $p \mid b$ or $p \mid c$. Suppose $p \mid b$. Then $b = px$ for some $x \in R$. This implies that $p = pxc$, i.e., $p(1 - xc) = 0$. Since R is an integral domain and $p \neq 0$, we have $xc = 1$ and so c is a unit in R. Similarly, one can show that if $p \mid c$, then b is a unit. Therefore p is irreducible. □

Before proceeding further, let us concentrate our discussion on the ring $\mathbb{Z}[\sqrt{-5}] = \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. It is a subring (with identity) of the field of complex numbers. Hence $\mathbb{Z}[\sqrt{-5}]$ is an integral domain. In the following, we show some interesting properties of elements of $\mathbb{Z}[\sqrt{-5}]$:

(i) 1 and -1 are the only units of $\mathbb{Z}[\sqrt{-5}]$: We show that an element $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ is a unit if and only if $a^2+5b^2 = 1$. Suppose $a+b\sqrt{-5}$ is a unit. Then there exists an element $c+d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ such that $(a+b\sqrt{-5})(c+d\sqrt{-5}) = 1$. Then $\overline{(a+b\sqrt{-5})(c+d\sqrt{-5})} = \bar{1}$, where $\bar{\alpha}$ denotes the conjugate of α in $\mathbb{C}$. Hence $(a-b\sqrt{-5})(c-d\sqrt{-5}) = 1$, whence we have $1 = (a+b\sqrt{-5})(c+d\sqrt{-5})(a-b\sqrt{-5})(c-d\sqrt{-5}) = (a^2+5b^2)(c^2+5d^2)$. Since $a, b, c, d \in \mathbb{Z}$, we find that $a^2+5b^2 = 1$.

[1]That is, p has no *proper* divisor. For $a, b \in R$ with $b \mid a$, b is called a *proper divisor* of a if b is neither an associate of a nor a unit.

IMS
(INSTITUTE OF MATHEMATICAL SCIENCES)
INSTITUTE FOR IAS/IFoS EXAMINATION
NEW DELHI-110009
Mob: 09999197625

Factorization in Integral Domains

13.1 Factorization Domain

In this section, we begin by introducing the concept of divisibility in an arbitrary commutative ring and then concentrate mainly on integral domains. As usual our natural inspiration is the ring of integers, $\mathbb{Z}$. For any two integers a and b (say), a is said to divide b if and only if there exists an integer c such that $ac = b$. An abstraction of this idea leads us to define the following:

Definition 13.1.1 Let R be a commutative ring with identity. Let $a, b \in R$ such that $a \neq 0$. Then a is said to *divide* b if there exists $c \in R$ such that $ac = b$. We write $a \mid b$. In this case, a is called a *divisor* of b. If $a \mid b$ and $b \mid a$, then a and b are called *associates*. We write $a \sim b$.

Note that 1 is a divisor of any element $a \in R$ and every nonzero element of R divides 0. If u is a unit in R, then $u \mid 1$ and hence $u \mid a$ for all $a \in R$. In the ring $\mathbb{Z}$, $2 \sim -2$. In general, $n \sim -n$ for all $n \in \mathbb{Z} \setminus \{0\}$. Recall that the principal ideal generated by an element $a \in R$ is denoted by (a). Then the following theorem is obvious.

Theorem 13.1.2 *Let R be a commutative ring with identity and $a, b, u \in R \setminus \{0\}$. Then*

(i) $a \mid b \iff b \in (a) \iff (b) \subseteq (a)$;

Solution. Let $I = \langle\{2, x\}\rangle$, i.e., I be the ideal in $\mathbb{Z}[x]$ generated by elements 2 and x. We show that I is not a principal ideal. Suppose, if possible, $I = \langle f(x)\rangle$ for some polynomial $f(x)$ in $\mathbb{Z}[x]$. Now, $2 \in I = \langle f(x)\rangle$ implies that there exists $g_1(x) \in \mathbb{Z}[x]$ such that $2 = f(x)g_1(x)$. But this shows $\deg f(x) = 0$, i.e., $f(x)$ is a constant, say a. So $x \in I = \langle f(x)\rangle = \langle a\rangle$. Then there is a polynomial $g_2(x) \in \mathbb{Z}[x]$ so that $x = ag_2$ which implies that $a = 1$ or -1.

In either case, $I = \mathbb{Z}[x]$. Therefore $1 \in I = \langle\{2, x\}\rangle$. Then there are $g(x), h(x) \in \mathbb{Z}[x]$ such that $1 = 2g(x) + xh(x)$ which is a contradiction as the constant term on the right hand side is an even integer, whereas that on the left hand side is 1. Therefore I cannot be a principal ideal in $\mathbb{Z}[x]$. Hence $\mathbb{Z}[x]$ is not a PID.

Exercises

1. Determine all the associates of [3] in $\mathbb{Z}_{10}$.
2. In $\mathbb{Z}[\sqrt{3}]$, show that $2+\sqrt{3}$ is a unit and $3+2\sqrt{3}$ is an associate of 3.
3. Determine all the units of $\mathbb{Z}[i]$.
4. Determine all the associates of $8+3i$ in $\mathbb{Z}[i]$.
5. Determine all units of $\mathbb{Z}[i\sqrt{3}]$. Show that $2, 1+i\sqrt{3}$ are irreducible in $\mathbb{Z}[i\sqrt{3}]$ but not prime.
6. Find all the units of $\mathbb{Z}_7[x]$. Also determine all the associates of $x^2+[2]$ in $\mathbb{Z}_7[x]$.
7. Find all associates of $1+i$ in $\mathbb{Z}[i]$.
8. Determine whether the following elements are prime or irreducible or none of them, in respect of the rings associated with them:
   (i) [2], [3], [4], [7], [9], [10] in $\mathbb{Z}_{12}$.
   (ii) $2, 4+\sqrt{10}$ in $\mathbb{Z}[\sqrt{10}]$.
   (iii) $3, 5, 11, 2+i, 3+i, 2-i, 1-i$ in $\mathbb{Z}[i]$.
   (iv) $23, 1+i3\sqrt{5}, 3+i\sqrt{5}, 2+i\sqrt{5}, 7+i3\sqrt{5}$ in $\mathbb{Z}[i\sqrt{5}]$.
9. Let D be a commutative ring with identity. If p be a prime element of D such that $p \mid a_1a_2\ldots a_n$ $(n \geq 2)$, $a_i \in D$. Then prove that $p \mid a_i$ for some $i \in \{1, 2, \ldots, n\}$.
10. Prove that $a+ib$ is prime in $\mathbb{Z}[i]$, if a^2+b^2 is prime in $\mathbb{Z}$.
11. Prove that $a+ib\sqrt{3}$ is irreducible in $\mathbb{Z}[i\sqrt{3}]$, if a^2+3b^2 is prime in $\mathbb{Z}$.
12. In $\mathbb{Z}[\sqrt{5}]$, show that 2 and $1+\sqrt{5}$ are irreducible but not prime.
13. In $\mathbb{Z}[\sqrt{-5}]$, show that the factorization of 21 as a product of irreducible elements is not unique.

14. Let p be a prime number of the form $4n+1$. Prove that $p = a^2+b^2$ for some $a, b \in \mathbb{Z}$ and p is not prime in $\mathbb{Z}[i]$. Also show that an integer m is a prime element in $\mathbb{Z}[i]$ if m is a prime number of the form $4n+3$.
15. Let $I \neq (0)$ be an ideal of $\mathbb{Z}[i]$. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite.
16. Let $I \neq \{0\}$ be a proper ideal of a PID R such that the quotient ring R/I has no nonzero zero divisors. Prove that R/I is a field.
17. Prove that the integral domains $\mathbb{Z}[i\sqrt{n}]$ for $n = 6, 7, 10$ are FD but not UFD.
18. Let R be a UFD and $d \in R \setminus \{0\}$. Show that the number of principal ideals containing d is finite.
19. Determine whether the following statements are true or false. Justify your answer.
   (i) 3 is an irreducible element in $\mathbb{Z}[i]$.
   (ii) 5 is an irreducible element in $\mathbb{Z}[i]$.
   (iii) 13 is an irreducible element in $\mathbb{Z}[i]$.
   (iv) $1+i$ is irreducible element in $\mathbb{Z}[i]$.
   (v) Every prime element of $\mathbb{Z}$ is also a prime element in $\mathbb{Z}[i]$.
   (vi) In $\mathbb{Z}[\sqrt{2}]$, $2+\sqrt{2}$ and $\sqrt{2}$ are associates.
   (vii) 3 is a prime in $\mathbb{Q}$.
   (viii) $\sqrt{3}$ is irreducible in $\mathbb{R}$.
   (ix) In $\mathbb{Z}_4$, [2] is an irreducible element.

13.2 Euclidean Domain

In this section, we define another important class of integral domains. Euclidean division algorithm is very much well-known to us from the beginning of learning the method of division in our school days, which states: dividend = divisor × quotient + remainder. Apart from the ring of integers, there are many integral domains in which the division algorithm holds. They are called Euclidean domains.

Definition 13.2.1. An integral domain R is called a *Euclidean domain* (in short, *ED*), if there exists a function $\delta : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ satisfying the following conditions:

(i) $\delta(a) \leq \delta(ab)$ for all $a, b \in R \setminus \{0\}$;

(ii) for any $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ (called respectively, *quotient* and *remainder*) such that

$$a = bq + r, \quad \text{where either } r = 0 \text{ or } \delta(r) < \delta(b).$$

The function δ is called a *Euclidean norm function* (or *Euclidean valuation*) on R.

Remark 13.2.2. First note that, for any $a \in R \smallsetminus \{0\}$, $\delta(a) \le \delta((-1)a) = \delta(-a)$, which in turn implies that $\delta(-a) \le \delta(-(-a)) = \delta(a)$ and so we have $\delta(a) = \delta(-a)$ for all $a \in R \smallsetminus \{0\}$.

Secondly, for any $a \in R \smallsetminus \{0\}$, $\delta(1) \le \delta(1 \cdot a) = \delta(a)$. Thus $\delta(1)$ is the least element in the subset $\delta(R \smallsetminus \{0\})$ of the well-ordered set, $\mathbb{N}_0$.

Finally, the group of units of R is precisely the set

$$\{u \in R \mid \delta(u) = \delta(1)\} \quad \text{(cf. Worked out Exercise 13.2.1).}$$

Example 13.2.3. Any field F is a Euclidean domain with $\delta(a) = 1$ for all $a \in F \smallsetminus \{0\}$. Note that, for all $a, b \in F \smallsetminus \{0\}$, $ab \neq 0$ and then $\delta(a) = 1 = \delta(ab)$ and for any $c \in F$, $c = (ca^{-1})a + 0$.

Example 13.2.4. The ring of integers, $\mathbb{Z}$ is a Euclidean domain with $\delta(a) = |a|$ for all $a \in \mathbb{Z} \smallsetminus \{0\}$. Note that for any $a, b \in \mathbb{Z} \smallsetminus \{0\}$, $|a| \le |ab|$ and for any $a \in \mathbb{Z}$, $b \in \mathbb{Z} \smallsetminus \{0\}$, there exist $q, r \in \mathbb{Z}$ such that $a = bq + r$ where either $r = 0$ or $|r| < |b|$.

Example 13.2.5. (Ring of Gaussian integers). The ring $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ is called the ring of Gaussian integers (cf. Example 11.1.5). Define $\delta(a + ib) = |a + ib|^2 = a^2 + b^2$ for all $a + ib \in \mathbb{Z}[i] \smallsetminus \{0\}$. Clearly, $\delta(u) > 0$ for all $u \neq 0$ in $\mathbb{Z}[i]$. Further for any $u, v \in \mathbb{Z}[i] \smallsetminus \{0\}$, $\delta(uv) = |uv|^2 = |u|^2|v|^2 \ge |u|^2 = \delta(u)$ since $|v|^2$ is sum of squares of two integers (both of which are not simultaneously zero).

Next let $u, v \in \mathbb{Z}[i]$ with $v \neq 0$. Then $u = a + ib$ and $v = c + id$ for some $a, b, c, d \in \mathbb{Z}$ such that $(c, d) \neq (0, 0)$. Now,

$$\frac{u}{v} = \frac{(a + ib)(c - id)}{c^2 + d^2} = \alpha + i\beta \quad \text{(say)},$$

where α, β are rational numbers. Then there exist integers m and n such that $|m - \alpha| \le \frac{1}{2}$ and $|n - \beta| \le \frac{1}{2}$. So $u = (\alpha + i\beta)v = (m + in)v + [(\alpha - m) + i(\beta - n)]v$. Now $[(\alpha - m) + i(\beta - n)]v = u - (m + in)v \in \mathbb{Z}[i]$, as $\mathbb{Z}[i]$ is a ring and $u, v, m + in \in \mathbb{Z}[i]$. Let $r = [(\alpha - m) + i(\beta - n)]v$. Then

$$\delta(r) = |r|^2 = [(\alpha - m)^2 + (\beta - n)^2]|v|^2 \le (\tfrac{1}{4} + \tfrac{1}{4})|v|^2 = \tfrac{1}{2}|v|^2 < |v|^2 = \delta(v).$$

Thus taking $q = m + in$, we have $u = vq + r$ where either $r = 0$ or $\delta(r) < \delta(v)$. Hence $\mathbb{Z}[i]$ is a Euclidean domain.

Theorem 13.2.6. *Every Euclidean domain is a PID.*

Proof. Let R be a Euclidean domain with a Euclidean valuation δ. Suppose I is a nonzero ideal of R. Let

$$T = \{\delta(x) \in \mathbb{N}_0 \mid x \neq 0,\ x \in I\}.$$

Clearly, T is a nonempty subset of $\mathbb{N}_0$. Then by the well-ordering principle, T has a least element. So, there exists a nonzero element $a \in I$ such that $\delta(a)$ is the least element in T. If $b \in I$, then $b = aq + r$ for some $q, r \in R$ where either $r = 0$ or $\delta(r) < \delta(a)$.

Now $r = b - aq \in I$, as $a, b \in I$. If $r \neq 0$, then $\delta(r) \ge \delta(a)$ by the choice of the element a in I. So $r = 0$ and hence $b = aq \in (a)$. Thus $I \subseteq (a)$. Also since $a \in I$, we have $I = (a)$. Therefore R is a PID. □

The following example shows that the converse is not true.

Example 13.2.7. Let R be the ring defined by

$$R = \left\{a + b(1 + i\sqrt{19})/2 \mid a, b \in \mathbb{Z}\right\}.$$

Then R is a PID but not a Euclidean domain.[5]

Thus we have the following:

$$\text{Euclidean domain} \Longrightarrow \text{PID} \Longrightarrow \text{UFD}$$

But the converse implications do not hold.

Now we shall define the greatest common divisor and the least common multiple in an arbitrary commutative ring with identity.

Definition 13.2.8. Let R be a commutative ring with identity. Let $a, b \in R$ such that a and b are not both zero. An element $d \in R$ is called a *greatest common divisor* (in short, *gcd*) or *highest common factor* (in short, *hcf*) of a and b if

(i) $d \mid a$ and $d \mid b$;

(ii) $x \mid a,\ x \mid b,\ x \in R \Longrightarrow x \mid d$.

[5] The proof is beyond the scope of the book. However one may find a proof in J. C. Wilson, *A principal ideal ring that is not a Euclidean ring*, *Mathematics Magazine* 46 (1973), 34-38.

We write $d = \gcd(a,b)$ or sometimes simply (a,b). The elements a and b are called *relatively prime* or *prime to each other* if $\gcd(a,b)$ is a unit (i.e., $\gcd(a,b) \sim 1$).

Similarly, let $a, b \in R$ such that $a, b \neq 0$. Then an element $c \in R$ is called a *least common multiple* (in short, *lcm*) of a and b if

(i) $a \mid c$ and $b \mid c$;

(ii) $a \mid y$, $b \mid y$, $y \in R \Longrightarrow c \mid y$.

We write $c = \text{lcm}(a,b)$ or simply $[a,b]$.

It is important to understand that in general, $\gcd(a,b)$ may or may not exist. But if a gcd exists, then it is unique up to associates, i.e., if x and y both are greatest common divisors of a and b, then $x \sim y$. The same is true for lcm also. For example, we consider the following:

Example 13.2.9. In $\mathbb{Z}$, both 3 and -3 are the greatest common divisors of 6 and 9. Similarly 18 and -18 are the least common multiples of them. Clearly, $3 \sim -3$ and $18 \sim -18$.

Theorem 13.2.10. *If R is a UFD, then there exists a gcd for any $a, b \in R \setminus \{0\}$.*

Proof. If a or b is a unit, then $\gcd(a,b) = 1$. Suppose a and b are non-units. Then both of them can be uniquely (up to associates) expressed as finite products of irreducible elements. Moreover we can express each of these products in terms of the same set of irreducible elements as

$$a \sim p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \text{ and } b \sim p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$$

where p_i's are "distinct" irreducible elements (in the sense that $p_i \sim p_j$ if and only if $i \neq j$) and r_i, s_i are nonnegative integers such that $r_i = 0$ [$s_i = 0$] if and only if p_i was not associated with any of the irreducible factors in the original expression of a [resp. b].

Now it is an easy exercise to verify that

$$\gcd(a,b) = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$$

where $t_i = \min(r_i, s_i)$ for each $i = 1, 2, \ldots, n$. We leave this simple verification to the reader. □

Now since every Euclidean domain is a PID and every PID is a UFD, the above theorem is also true for these classes of domains. But in the case of a PID (and hence also for a Euclidean domain) we have something more.

Theorem 13.2.11. *Let R be a PID [and hence a Euclidean domain] and $a, b \in R \setminus \{0\}$. Then there exists $\gcd(a,b)$. Also if $d = \gcd(a,b)$, then there exist $x, y \in R$ such that $d = ax + by$.*

Proof. We prove the result only for a PID and then it follows for a Euclidean domain also.

Let I be the ideal generated by $\{a, b\}$. Then $I = Ra + Rb$. Now since R is a PID, $I = (d)$ for some $d \in R$. Thus there exist $x, y \in R$ such that $d = ax + by$. Since $a, b \in I = (d)$, we have $d \mid a$ and $d \mid b$. Also, if there is some $c \in R$ so that $c \mid a$ and $c \mid b$, then $c \mid (ax + by) = d$. Therefore $d = \gcd(a,b)$. Hence there exists $\gcd(a,b) = d$ and $d = ax + by$ for some $x, y \in R$. □

The method of finding the gcd in a Euclidean domain is known as *Euclidean algorithm*. In the following, we shall describe it[6]:

Let R be a Euclidean domain and $a, b \in R$ such that a, b are not both zero. If $b = 0$, then $a = \gcd(a,b)$. Suppose $b \neq 0$. Then we have $q, r \in R$ such that $a = bq + r$ where either $r = 0$ or $\delta(r) < \delta(b)$. If $r = 0$, then clearly $b = \gcd(a,b)$. If $r \neq 0$, let $d = \gcd(b,r)$. Then $d \mid b$ and $d \mid r$, which implies that $d \mid (bq + r) = a$. Also if $x \in R$ be such that $x \mid a$ and $x \mid b$, then $x \mid (a - bq) = r$. This implies that $x \mid d$ as $d = \gcd(b,r)$. Hence $d = \gcd(a,b)$.

Now consider the elements b and r and by applying the division algorithm for them we get $q_1, r_1 \in R$ so that $b = rq_1 + r_1$ where either $r_1 = 0$ or $\delta(r_1) < \delta(r)$. If $r_1 = 0$, then $r \mid b$ and hence $r = \gcd(b,r) = \gcd(a,b)$. Otherwise, $r_1 \neq 0$ and we continue the process to obtain

$$\begin{aligned} a &= bq + r, &\quad \text{where } \delta(r) < \delta(b) \\ b &= rq_1 + r_1, &\quad \text{where } \delta(r_1) < \delta(r) \\ r &= r_1 q_2 + r_2, &\quad \text{where } \delta(r_2) < \delta(r_1) \end{aligned}$$

[6] One can easily recognize the method. It is exactly the same as what we did in our school days,

The above process must terminate after a finite number of steps, since $\delta(b)$ is a positive integer and there exist finite number of distinct positive integers less than $\delta(b)$. Thus, finally we have

$$r_{n-1} = r_n q_{n+1}$$

for some n, i.e., at some stage the remainder $r_{n+1} = 0$, for otherwise the values of $\delta(r_i)$ go on decreasing indefinitely. So we have

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_{n-1},r_n) = r_n.$$

Also using the equalities obtained above, one can easily compute $x, y \in R$ so that $\gcd(a,b) = ax + by$. This is illustrated in Worked Out Exercise 13.2.5. For a better understanding, the reader is asked to go through Example 2.1.11 again.

Worked Out Exercises

◇ **Exercise 13.2.1.** Let R be a Euclidean domain with the Euclidean norm δ. Let $u \in R \setminus \{0\}$. Prove that u is a unit in R if and only if $\delta(u) = \delta(1)$.

Solution. If u is a unit, then there exists $v \in R$ so that $uv = 1$. Then $\delta(u) \leqslant \delta(uv) = \delta(1)$. But $\delta(1) \leqslant \delta(u)$. This implies that $\delta(u) = \delta(1)$.

Conversely, let $\delta(u) = \delta(1)$. Now since R is a Euclidean domain, we have that there are $q, r \in R$ such that $1 = qu + r$ where $r = 0$ or $\delta(r) < \delta(u)$. Since $\delta(u) = \delta(1) \leqslant \delta(r)$, we have $r = 0$. Thus, $1 = qu$ which implies that u is a unit in R.

◇ **Exercise 13.2.2.** Let R be a Euclidean domain with the Euclidean norm δ. Let $a, b \in R \setminus \{0\}$. Prove that b is a unit in R if and only if $\delta(a) = \delta(ab)$ (i.e., b is not a unit in R if and only if $\delta(a) < \delta(ab)$ for all $a \in R \setminus \{0\}$).

Solution. Suppose b is a unit in R. Then $\delta(ab) \leqslant \delta(abb^{-1}) = \delta(a)$. Also $\delta(a) \leqslant \delta(ab)$. Therefore $\delta(a) = \delta(ab)$.

Conversely, suppose $\delta(a) = \delta(ab)$. Now by the Euclidean property of R, we have that there are $q, r \in R$ such that $a = qab + r$ where $r = 0$ or $\delta(r) < \delta(ab)$. If $r \neq 0$, then $r = a(1-qb) \neq 0$. This implies that $\delta(ab) = \delta(a) \leqslant \delta(a(1-qb)) = \delta(a-qab) = \delta(r)$. Thus $r = 0$. So $a(1-qb) = a - aqb = 0$ which implies that $1 - qb = 0$ as $a \neq 0$ and R is an integral domain. Therefore $qb = 1$ and hence b is a unit in R.

◇ **Exercise 13.2.3.** Prove that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.

Solution. Define $\delta(a + b\sqrt{2}) = |a^2 - 2b^2|$ for all $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$. Clearly, $\delta(u) \geqslant 0$ for all $u \neq 0$ in $\mathbb{Z}[\sqrt{2}]$. Also verify that $a^2 - 2b^2 = 0$ if and only if $a = b = 0$ as $a, b \in \mathbb{Z}$. Thus $\delta(u) \geqslant 1$ for all $u \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$. Further, for any $u = a + b\sqrt{2}, v = c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$, $\delta(uv) = \delta((ac + 2bd) + (bc + ad)\sqrt{2}) = |(ac + 2bd)^2 - 2(bc + ad)^2| = |a^2c^2 + 4abcd + 4b^2d^2 - 2(b^2c^2 + 2abcd + a^2d^2)| = |a^2c^2 + 4b^2d^2 - 2b^2c^2 - 2a^2d^2| = |(a^2 - 2b^2)(c^2 - 2d^2)| = \delta(u)\delta(v) \geqslant \delta(u)$ as $\delta(v) \geqslant 1$.

Next let $u, v \in \mathbb{Z}[\sqrt{2}]$ with $v \neq 0$. Then $u = a + b\sqrt{2}$ and $v = c + d\sqrt{2}$ for some $a, b, c, d \in \mathbb{Z}$ such that $(c, d) \neq (0, 0)$. Now,

$$\frac{u}{v} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = \alpha + \beta\sqrt{2} \quad \text{(say)},$$

where α, β are rational numbers. Then there exist integers m and n such that $|m - \alpha| \leq \frac{1}{2}$ and $|n - \beta| \leq \frac{1}{2}$. So

$$u = (\alpha + \beta\sqrt{2})v = (m + n\sqrt{2})v + [(\alpha - m) + (\beta - n)\sqrt{2}]v.$$

Now $[(\alpha - m) + (\beta - n)\sqrt{2}]v = u - (m + n\sqrt{2})v \in \mathbb{Z}[\sqrt{2}]$, as $\mathbb{Z}[\sqrt{2}]$ is a ring and $u, v, m + n\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Let $r = [(\alpha - m) + (\beta - n)\sqrt{2}]v$. Then $\delta(r) = |(\alpha - m)^2 - 2(\beta - n)^2||c^2 - 2d^2| \leq (\frac{1}{4} + \frac{2}{4})|c^2 - 2d^2| = \frac{3}{4}|c^2 - 2d^2| < |c^2 - 2d^2| = \delta(v)$. Thus taking $q = m + n\sqrt{2}$, we have $u = vq + r$ where either $r = 0$ or $\delta(r) < \delta(v)$. Hence $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

▶ **Exercise 13.2.4.** Determine all the prime elements of $\mathbb{Z}[i]$.

Solution. We first note that since $\mathbb{Z}[i]$ is a Euclidean domain (cf. Example 13.2.5), prime and irreducible elements of $\mathbb{Z}[i]$ are the same. Also, the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ (cf. Problem 3 of Exercise 13.1). Let $z = a + ib$ be an irreducible (or prime) element in $\mathbb{Z}[i]$. Then, associates of z are $\pm z$ and $\pm iz$ which are also primes in $\mathbb{Z}[i]$.

Now if $b = 0$, i.e., $z = a \in \mathbb{Z}$. Then z must be a prime number, for otherwise z has a nontrivial factorization in $\mathbb{Z}$ and hence in $\mathbb{Z}[i]$. But not all prime numbers are prime elements in $\mathbb{Z}[i]$. For example, $5 = (2 + i)(2 - i)$. In fact, by Problem 14 of Exercise 13.1, we know that $z \in \mathbb{Z}$ is a prime element of $\mathbb{Z}[i]$ if and only if z is of the form $4n + 3$. Therefore, in this case, $z = \pm p$ where p is a prime number of the form $4n + 3$.

Let $b \neq 0$. If $a = 0$, then $z = ib$ and so $b \in \mathbb{Z}$ is an associate of z. So we have $z = \pm ip$ where p is a prime number of the form $4n + 3$.

Let $a, b \neq 0$. Then $\bar{z} = a - ib$ is also irreducible. For if $\bar{z} = z_1 z_2$ be a nontrivial factorization of $\bar{z}$, then $z = \overline{z_1}\,\overline{z_2}$ is also a nontrivial factorization of z. Therefore, $a^2 + b^2 = z\bar{z}$ is a factorization of $a^2 + b^2$ in $\mathbb{Z}[i]$ in terms of irreducible factors which is unique up to associates as $\mathbb{Z}[i]$, being an Euclidean domain, certainly a UFD. This at once follows that $a^2 + b^2$ is a prime integer because any nontrivial factorization of $a^2 + b^2$ in terms of prime integers would be a different from the one that we already have.

Conversely, arguing as in Exercise 13.1.4, one can show that, if $a^2 + b^2$ is a prime integer, then $a + ib$ is prime in $\mathbb{Z}[i]$. Hence, in this case, $z = a + ib$, $(a, b \neq 0)$ is prime in $\mathbb{Z}[i]$ if and only if $a^2 + b^2$ is a prime number.

◊ Exercise 13.2.5. Find the gcd of $-3 + 11i$ and $8 - i$ in $\mathbb{Z}[i]$. Also find $x, y \in \mathbb{Z}[i]$ such that $\gcd(-3 + 11i, 8 - i) = (-3 + 11i)x + (8 - i)y$.

Solution. We shall follow the Euclidean algorithm. We have $\frac{-3+11i}{8-i} = \frac{(-3+11i)(8+i)}{65} = \frac{-35+85i}{65} = -\frac{7}{13} + \frac{17}{13}i = (-1 + i) + \left(\frac{6}{13} + \frac{4}{13}i\right) = (-1 + i) + \frac{2}{13}(3 + 2i)$. Thus $-3 + 11i = (-1 + i)(8 - i) + \frac{2}{13}(3 + 2i)(8 - i) = (-1 + i)(8 - i) + \frac{2}{13}(26 + 13i)$. Therefore,

$$-3 + 11i = (-1 + i)(8 - i) + (4 + 2i). \tag{13.2.1}$$

Again, $\frac{8-i}{4+2i} = \frac{(8-i)(4-2i)}{20} = \frac{30-20i}{20} = \frac{3}{2} - i = (1 - i) + \frac{1}{2}$. Then we have

$$8 - i = (1 - i)(4 + 2i) + (2 + i). \tag{13.2.2}$$

Finally, $\frac{4+2i}{2+i} = 2$ and so $4 + 2i = 2(2 + i)$. Therefore, $\gcd(-3 + 11i, 8 - i) = 2 + i$.

Now to find the desired values of x and y, we use the above equations and proceed as follows:

$$\begin{aligned} 2 + i &= (8 - i) - (1 - i)(4 + 2i) \quad \text{by (13.2.2)} \\ &= (8 - i) - (1 - i)\{(-3 + 11i) - (-1 + i)(8 - i)\} \quad \text{by (13.2.1)} \\ &= (-1 + i)(-3 + 11i) + \{1 + (1 - i)(-1 + i)\}(8 - i) \\ &= (-1 + i)(-3 + 11i) + (1 + 2i)(8 - i). \end{aligned}$$

Thus $x = -1 + i$ and $y = 1 + 2i$.[7]

◊ Exercise 13.2.6. Prove that 2 and $1 + i\sqrt{5}$ are relatively prime in the integral domain $\mathbb{Z}[i\sqrt{5}]$.

[7] Note that the values of x and y are not unique.

6

Solution. We know that only units of $\mathbb{Z}[i\sqrt{5}]$ are 1 and -1. Suppose $a + ib\sqrt{5}$ is a common divisor of 2 and $1 + i\sqrt{5}$. Then $2 = (a + ib\sqrt{5})(c + id\sqrt{5})$ for some $c + id\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$. So we have

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Now since $a, b, c, d \in \mathbb{Z}$, we have $a^2 + 5b^2 = 1, 2$ or 4. Also note that since $a, b \in \mathbb{Z}$, $a^2 + 5b^2 \neq 2$ and $a^2 + 5b^2 = 4$ implies that $a = \pm 2$ and $b = 0$. Therefore in this case, $a + ib\sqrt{5} = 2$ divides $1 + i\sqrt{5}$. Then there exists $u + iv\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ such that $(1 + i\sqrt{5}) = 2(u + iv\sqrt{5})$. But this implies that $2u = 1$ which is a contradiction as $u \in \mathbb{Z}$.

Therefore $a^2 + 5b^2 = 1$, which implies that $a = \pm 1$ and $b = 0$. Thus the only common divisors of 2 and $1 + i\sqrt{5}$ are 1 and -1. Hence 2 and $1 + i\sqrt{5}$ are relatively prime in $\mathbb{Z}[i\sqrt{5}]$.

◊ Exercise 13.2.7. In a UFD R, for any $a, b \neq 0$ prove that $ab \sim \gcd(a, b)\,\mathrm{lcm}(a, b)$.

Solution. Let d be a gcd of a and b respectively. Let $a = dx$ and $b = dy$. We show that $c = dxy$ is the lcm of a and b. Clearly $a \mid c$ and $b \mid c$. Let $u \in R$ such that $a \mid u$ and $b \mid u$. Then $dx \mid u$ and since $y \mid b$, we also have $y \mid u$. Thus $c = dxy \mid u$. Therefore c is a lcm of a and b.

Now $ab = dx \cdot dy = d^2xy = dc$. Also since any two gcds are associates and the same is true for lcms, we have $ab \sim \gcd(a, b)\,\mathrm{lcm}(a, b)$ as required.

◊ Exercise 13.2.8. Prove that in a PID, every nonzero proper ideal can be expressed uniquely (up to order) as a finite product of prime ideals.

Solution. Let R be a PID and I be a nonzero proper ideal of R. Then $I = (a)$ for some nonzero nonunit element $a \in R$. Since any PID is a UFD by Theorem 13.1.21, we have

$$a = a_1 a_2 \ldots a_n, \tag{13.2.3}$$

where each $a_i \in R$ is irreducible and hence prime. Let $M_i = (a_i)$ for each i. Also by Theorem 13.1.9, each M_i is a prime ideal of R. We show that $I = M_1 M_2 \ldots M_n$. Clearly, it follows from (13.2.3) that $a \in M_1 M_2 \ldots M_n$ and hence $I = (a) \subseteq M_1 M_2 \ldots M_n$.

Conversely, let $x \in M_1 M_2 \ldots M_n$. Then,

$$x = \sum_{i}^{m} b_{1i} b_{2i} \ldots b_{ni}$$

where $b_{ik} \in M_i$ for all $i = 1, 2, \ldots, n$. Now since $M_i = (a_i)$, we have for each i and for each k, $b_{ik} = a_i x_{ik}$ for some $x_{ik} \in R$. Thus for each k, $b_{1k}b_{2k}\ldots b_{nk} = a_1 a_2 \ldots a_n x_{1k} x_{2k} \ldots x_{nk} = a x_{1k} x_{2k} \ldots x_{nk} \in I$. This implies that

$$x = \sum_{k=1}^{m} b_{1k} b_{2k} \ldots b_{nk} \in I.$$

Therefore $I = M_1 M_2 \ldots M_n$ as required.

Exercises

1. Let R be a Euclidean domain with a Euclidean norm δ. Prove that $\delta(a) = \delta(-a)$ for all nonzero elements a in R.
2. Let R be a Euclidean domain with a Euclidean norm δ and $a, b \in R \setminus \{0\}$ such that $a \sim b$. Show that $\delta(a) = \delta(b)$. Conversely, if $\delta(a) = \delta(b)$ for some $a, b \in R \setminus \{0\}$ so that either $a \mid b$ or $b \mid a$, then show that $a \sim b$.
3. Show that for each positive integer n, $\delta(a) = |a|^n$ is a Euclidean norm on $\mathbb{Z}$.
4. Prove that $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ is a Euclidean domain.
5. Prove that $\mathbb{Z}[\sqrt{n}]$ is a Euclidean domain for $n = -1$ and $n = -2$.
6. Let $a, b \in \mathbb{Z}[\sqrt{3}]$ where $a = -102 + 10\sqrt{3}$ and $b = 1 + 7\sqrt{3}$. Find $q, r \in \mathbb{Z}[\sqrt{3}]$ so that $a = bq + r$, where either $r = 0$ or $r = \alpha + \beta\sqrt{3}$ with $|\alpha^2 - 3\beta^2| < 146$.
7. In a UFD R, let $a, b \in R \setminus \{0\}$, prove that any two greatest common divisors of a and b are associates.
8. In a UFD R, let $a, b, c \in R \setminus \{0\}$. If $a \mid bc$ and $\gcd(a, b) \sim 1$, then show that $a \mid c$.
9. Let R be a UFD and $a, b, c \in R \setminus \{0\}$. Show that $\gcd(ca, cb) \sim c \gcd(a, b)$.
10. Let R be a UFD and $a, b \in R \setminus \{0\}$. Prove that there exists a lcm of a and b in R.
11. Let R be a commutative ring with identity and $a_1, a_2, \ldots, a_n \in R \setminus \{0\}$. Define (inductively), gcd and lcm of $a_1, a_2, \ldots, a_n$. Prove that they exist if R is a UFD.
12. Let R be a Euclidean domain. Without using Theorem 13.2.10, prove that any two nonzero elements $a, b \in R$ have a gcd and $\gcd(a, b) = ax + by$ for some $x, y \in R$.
13. Find the gcd of $3 + i$ and $-5 + 10i$ in $\mathbb{Z}[i]$.
14. Find $x, y \in \mathbb{Z}[i]$ such that $\gcd(3 + i, -5 + 10i) = (3 + i)x + (-5 + 10i)y$.
15. Show that $2 + 11i$ and $2 - 7i$ are relatively prime in the integral domain $\mathbb{Z}[i]$.
16. Prove that in $\mathbb{Z}[i\sqrt{5}]$ gcd of $6(1 - i\sqrt{5})$ and $3(1 + i\sqrt{5})(1 - i\sqrt{5})$ does not exist.
17. Let R be a PID and $a, b, c \in R \setminus \{0\}$ such that $c = ax + by$ for some $x, y \in R$. Prove that $\gcd(a, b) \mid c$.
18. Let R be a Euclidean domain and $a, b \in R$ with $b \neq 0$. Let $q, r \in R$ so that $a = bq + r$ where $r \neq 0$. Prove that $\gcd(a, b) = \gcd(b, r)$.

7

Polynomial Rings

14.1 Ring of Polynomials

This section deals with a very important class of rings, namely, the ring of polynomials. Already we have seen that these rings provide examples and counter examples in a number of occasions. Now it is time to give a special attention to them, as this class of rings play a major role in the study of advanced ring theory, field theory and especially in the area of commutative algebra and algebraic geometry.

In Example 11.1.9, we have described the polynomial ring over a commutative ring with identity. Now we shall define it again in a more formal way and with some more rigor in order to establish the existence of it as an algebraic structure.

Throughout the chapter we assume that if a ring R contains 1, then $1 \neq 0$.

Definition 14.1.1 Let R be a commutative ring with identity. Let S be the set of all infinite sequences of elements of R, i.e.,

$$S = \{(a_0, a_1, a_2, a_3, \ldots, a_n, \ldots) \mid a_i \in R,\ i = 0, 1, 2, 3, \ldots\}.$$

Let T be the subset of S defined by

$$T = \{(a_0, a_1, a_2, a_3, \ldots, a_n, \ldots) \in S \mid a_i = 0 \text{ for all } i \geq n \text{ for some nonnegative integer } n\}.$$

Define addition and multiplication on T as follows:

$$(a_0, a_1, a_2, a_3, \ldots) + (b_0, b_1, b_2, b_3, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots), \quad (14.1.1)$$

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, c_3, \ldots), \quad (14.1.2)$$

where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{\substack{i,j=0 \\ i+j=k}}^{k} a_i b_j, \quad k = 0, 1, 2, 3, \ldots$$

In the following theorem, we shall prove that T becomes a ring with the binary operations defined above and in fact, it is again a commutative ring with identity. Now for convenience, we shall use the following notation with the help of a formal symbol x which will provide us a better (as well as more natural) description of the elements of T.

Denote $(a, 0, 0, 0, \ldots)$ by $a = ax^0$
$(0, a, 0, 0, \ldots)$ by $ax = ax^1$
$(0, 0, a, 0, \ldots)$ by ax^2
$(0, 0, 0, a, 0, \ldots)$ by ax^3
and so on,

for all $a \in R$. Thus in this notation ax^n (n being a nonnegative integer) represents the sequence $(a_0, a_1, a_2, a_3, \ldots)$ where $a_i = 0$ for all $i \neq n$ and $a_n = a$. Note that we are identifying x^0 with $1 \in R$ and x^1 with x. With this notation, a general element $(a_0, a_1, a_2, a_3, \ldots, a_n, 0, 0, \ldots) \in T$ can be written as $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$, as

$$\begin{aligned}(a_0, a_1, a_2, a_3, \ldots, a_n, 0, 0, \ldots) \\ = (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots) + (0, 0, a_2, 0, \ldots) \\ + (0, 0, 0, a_3, 0, \ldots) + (0, 0, \ldots, 0, a_n, 0, \ldots).\end{aligned}$$

This symbol x is called *indeterminate* over R, the general expression $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$ is called a *polynomial* over R in the indeterminate x and the elements a_i, $i = 0, 1, 2, \ldots, n$ are called *coefficients* of the above polynomial. Finally, the ring T is denoted by $R[x]$ and is called the *ring of polynomials* or the *polynomial ring* over R in the indeterminate x. Once this polynomial ring (of a single variable) is defined, one can easily extend it inductively for several indeterminates. Define $R[x, y] = (R[x])[y]$, where the later one is the polynomial ring over $R[x]$ in the indeterminate y. Similarly, we can define $R[x_1, x_2, x_3, \ldots, x_n]$ inductively by considering

$$R[x_1, x_2, \ldots, x_i] = (R[x_1, x_2, \ldots, x_{i-1}])[x_i]$$

for each $i = 2, 3, 4, \ldots, n$.

Remark 14.1.2. Note that in the above representation of elements of T in terms of polynomials, the element $(0, 1, 0, 0, \ldots)$ is denoted by $1x$ which we shall identify

with x. Also, for any $a \in R$, $ax = (a, 0, 0, \ldots)(0, 1, 0, 0, \ldots) = (0, a, 0, 0, \ldots) = (0, 1, 0, 0, \ldots)(a, 0, 0, \ldots) = xa$ by (14.1.2).

Again, since we have identified $ax^0 \in R[x]$ with $a \in R$, it is very important to understand that R is considered as a subring of $R[x]$. Finally, observe that two polynomials $a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$ and $b_0 + b_1x + b_2x^2 + b_3x^3 + \cdots + b_mx^m$ in $R[x]$ are equal if and only if $m = n$ and $a_i = b_i$ for all $i = 0, 1, 2, 3, \ldots, n$, which is evident from their equality as elements of T.

Theorem 14.1.3. *Let R be a commutative ring with identity. Then $R[x]$ (as defined above) is a commutative ring with identity and R is a subring of $R[x]$.*

Proof. We must prove the set T along with the binary operations defined by (14.1.1) and (14.1.2), forms a ring. Since addition is defined component wise, it is easy to verify that this addition is associative, commutative, that there is an additive identity, namely, the zero sequence, $\theta = (0, 0, 0, \ldots)$ (where all the entries are zero) and for each sequence $\sigma = (a_0, a_1, a_2, \ldots) \in T$, there exists a sequence $\sigma' = (-a_0, -a_1, -a_2, \ldots) \in T$ such that $\sigma + \sigma' = \theta$. All these verifications prove that $(T, +)$ is an abelian group.

Thus it remains to prove that the multiplication is associative, commutative, distributive over addition and there is a multiplicative identity. So let us choose any three elements σ, τ, η of T, where $\sigma = (a_0, a_1, a_2, \ldots)$, $\tau = (b_0, b_1, b_2, \ldots)$, $\eta = (c_0, c_1, c_2, \ldots)$. Then $\sigma\tau = (d_0, d_1, d_2, \ldots)$, where $d_l = \sum_{\substack{i,j=0 \\ i+j=l}} a_i b_j$, $l = 0, 1, 2, 3, \ldots$.
Since R is commutative, we have $d_l = \sum_{\substack{i,j=0 \\ i+j=l}} b_j a_i$, for all $l = 0, 1, 2, 3, \ldots$. This implies that $\sigma\tau = \tau\sigma$ for all $\sigma, \tau \in T$ and so the multiplication defined in (14.1.2) is commutative.

Again $(\sigma\tau)\eta = (e_0, e_1, e_2, \ldots)$, where $e_r = \sum_{\substack{l,k=0 \\ l+k=r}} d_l c_k$, $r = 0, 1, 2, 3, \ldots$. Thus $e_r = \sum_{\substack{i,j,k=0 \\ i+j+k=r}} a_i b_j c_k$. Similarly $\sigma(\tau\eta) = (f_1, f_2, f_3, \ldots)$, where $f_r = \sum_{\substack{i,l=0 \\ i+l=r}} a_i \left(\sum_{\substack{j,k=0 \\ j+k=l}} b_j c_k \right) = \sum_{\substack{i,j,k=0 \\ i+j+k=r}} a_i b_j c_k$, $r = 0, 1, 2, 3, \ldots$. Therefore $e_r = f_r$ for all $r = 0, 1, 2, 3, \ldots$. This implies that $(\sigma\tau)\eta = \sigma(\tau\eta)$ for all $\sigma, \tau, \eta \in T$ and hence the multiplication is associative.

Now let $\sigma(\tau+\eta) = (g_0, g_1, g_2, \ldots)$ and $\sigma\tau + \sigma\eta = (h_0, h_1, h_2, \ldots)$. Then $g_k = \sum_{\substack{i,j=0\\i+j=k}}^{k} a_i(b_j + c_j)$ and $h_k = \left(\sum_{\substack{i,j=0\\i+j=k}}^{k} a_ib_j\right) + \left(\sum_{\substack{i,j=0\\i+j=k}}^{k} a_ic_j\right) = \sum_{\substack{i,j=0\\i+j=k}}^{k} a_i(b_j + c_j)$ for $k = 0, 1, 2, 3, \ldots$. Thus $\sigma(\tau+\eta) = \sigma\tau + \sigma\eta$ for all $\sigma, \tau, \eta \in T$, which proves the distributive law.

Finally, it is easy to see that the sequence $(1, 0, 0, 0, \ldots)$ acts as an identity for the product (14.1.2). Therefore, T is a commutative ring with identity and identifying any element $a \in R$ with the sequence $(a, 0, 0, 0, \ldots) \in T$, we may consider R as a subring of T, which is denoted by $R[x]$. This completes the proof. □

Now let us explore some elementary properties of a polynomial ring over a commutative ring with identity.

Definition 14.1.4. Let R be a commutative ring with identity. Let $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n \in R[x]$ with $a_n \neq 0$. Then a_n is called the *leading coefficient* and n is called the *degree* of $f(x)$. In other words, degree of a polynomial $f(x)$ in $R[x]$ is the highest power of x in $f(x)$ and the leading coefficient[1] is the coefficient of the highest power of x in $f(x)$. We write $n = \deg f(x)$. If $a_n = 1$, then $f(x)$ is called *monic*. An element of R is also called a *constant polynomial*.

Proposition 14.1.5. *Let R be a commutative ring with identity and $f(x), g(x) \in R[x]$. Then,*

(i) $\deg(f(x)g(x)) \leq \deg f(x) + \deg g(x)$. The equality holds if R is an integral domain;

(ii) $\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$.

Proof. (i) Let $m = \deg f(x)$, $n = \deg g(x)$ and a_m, b_n be the leading coefficients of $f(x)$ and $g(x)$ respectively. Then $a_m, b_n \neq 0$. Now the expression of $f(x)g(x)$ terminates[2] with the term $a_mb_nx^{m+n}$. Thus the first part of (i) follows. Also if R is an integral domain, then $a_mb_n \neq 0$ and so in this case, $\deg(f(x)g(x)) = m + n = \deg f(x) + \deg g(x)$.

(ii) Obvious and left as an exercise. □

[1] Note that the leading coefficient is *always* nonzero, for otherwise the degree of the polynomial would be diminished.
[2] Considering as an element of T, all the entries after $(m+n+1)$-th. place are zero.

Theorem 14.1.6. (Division algorithm) *Let R be a commutative ring with identity. Let $f(x)$ and $g(x)$ be two polynomials in $R[x]$ such that the leading coefficient of $g(x)$ is a unit in R. Then there exist unique polynomials $q(x)$ and $r(x)$ in $R[x]$ (called quotient and remainder respectively) such that*

$$f(x) = q(x)g(x) + r(x),$$

where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Proof. If $f(x) = 0$, then $f(x) = 0 \cdot g(x) + 0$ proves the theorem. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, $a_n \neq 0$ and $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$, where b_m is a unit in R. If $n = m = 0$, then $f(x) = a_0$ and $g(x) = b_0$, which must then be a unit in R. So $f(x) = a_0 = (a_0b_0^{-1})b_0 = (a_0b_0^{-1})g(x) + 0$. Also if $n < m$, then $f(x) = 0 \cdot g(x) + f(x)$ with $\deg f(x) = n < m = \deg g(x)$. We proceed by induction on $\deg f(x) = n$. Assume that $n \geq m > 0$ and the division algorithm holds for all $f(x) \in R[x] \setminus \{0\}$ with $\deg f(x) < n$.

Let $f(x) \in R[x]$ such that $\deg f(x) = n$. Let $h(x) = f(x) - a_nb_m^{-1}x^{n-m}g(x)$. If $h(x) = 0$, then $f(x) = (a_nb_m^{-1}x^{n-m})g(x) + 0$. If $h(x) \neq 0$, then $\deg h(x) < n$ and so by induction hypothesis, $h(x) = q(x)g(x) + r(x)$ for some $q(x), r(x) \in R[x]$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. This implies that $f(x) = (q(x) + a_nb_m^{-1}x^{n-m})g(x) + r(x)$, where $r(x)$ has the same property as above. This completes the induction and proves the division algorithm in $R[x]$.

Now suppose $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, for some $q_i(x), r_i(x) \in R[x]$, where either $r_i(x) = 0$ or $\deg r_i(x) < \deg g(x)$, $(i = 1, 2)$. This implies that $\left(q_1(x) - q_2(x)\right)g(x) = r_2(x) - r_1(x)$. Now if $r_1(x) \neq r_2(x)$, then $0 \leq \deg\left(r_2(x) - r_1(x)\right) < \deg g(x)$. But since b_m is a unit, we have $\deg\left(r_2(x) - r_1(x)\right) = \deg\left(\left(q_1(x) - q_2(x)\right)g(x)\right) = \deg\left(q_1(x) - q_2(x)\right) + \deg g(x) \geq \deg g(x)$; which is a contradiction. Therefore $r_1(x) = r_2(x)$ and so $\left(q_1(x) - q_2(x)\right)g(x) = 0$. Again since b_m is a unit, the product cannot be identically zero unless $q_1(x) = q_2(x)$. Thus in this case, the quotient and the remainder of the division algorithm are unique. □

Definition 14.1.7. Let R be a commutative ring with identity and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$. For any $r \in R$, define

$$f(r) = a_0 + a_1r + a_2r^2 + \cdots + a_nr^n.$$

If $f(r) = 0$, then an element $r \in R$ is called a *root*[3] of $f(x)$.

[3] Also called a *zero* of $f(x)$.

Corollary 14.1.8. (Remainder Theorem) *Let R be a commutative ring with identity, $f(x) \in R[x]$ and $a \in R$. Then there exists $q(x) \in R[x]$ such that*

$$f(x) = (x-a)q(x) + f(a).$$

Proof. Since the leading coefficient of the polynomial $(x-a)$ is 1, by Theorem 14.1.6, we have that there exist $q(x), r(x) \in R[x]$ such that $f(x) = (x-a)q(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg(x-a) = 1$. Then $r(x)$ is a constant polynomial, i.e., $r(x) = r \in R$. Thus $f(x) = (x-a)q(x) + r$ which implies that $f(a) = (a-a)q(a) + r = r$. This completes the proof. □

Corollary 14.1.9. (Factorization Theorem) *Let R be a commutative ring with identity, $f(x) \in R[x]$ and $a \in R$. Then $(x-a)$ divides $f(x)$ if and only if a is a root of $f(x)$. (i.e., $f(a) = 0$).*[4]

Proof. Follows immediately from the remainder theorem (Corollary 14.1.8). □

Now, we shall study polynomial rings over some special classes of commutative rings with identity and the first one is an integral domain.

Theorem 14.1.10. *If R is an integral domain, then $R[x]$ is also an integral domain. In particular, if K is a field, then $K[x]$ is an integral domain.*

Proof. By Theorem 14.1.3, $R[x]$ is a commutative ring with 1_R. Let $f(x), g(x) \in R[x] \setminus \{0\}$ with the respective leading coefficients a_m and b_n. Then $a_m, b_n \neq 0$. As R is an ID, $a_m b_n \neq 0$ and it is the leading coefficient of the polynomial $f(x)g(x)$. Hence $f(x)g(x) \neq 0$. Thus $R[x]$ is also an integral domain. Rest is obvious. □

The converse of the above theorem is also true, since R is a subring of $R[x]$ which contains the identity. One can easily generalize the result as follows:

Corollary 14.1.11. *Let R be a commutative ring with identity. Then $R[x_1, x_2, x_3, \ldots, x_n]$ is an integral domain if and only if R is an integral domain.*

Proof. Follows from the repeated application of the above theorem. □

Next, it is natural to ask that: is there any special property for the polynomial ring over a field? The following theorem answers the question.

[4] The root $a \in R$ of $f(x) \in R[x]$ is said to be of multiplicity m if $(x-a)^m \mid f(x)$ but $(x-a)^{m+1} \nmid f(x)$.

Theorem 14.1.12. *If K is a field, then $K[x]$ is a Euclidean domain.*

Proof. By Theorem 14.1.10, $K[x]$ is an integral domain. Define $\delta : K[x] \setminus \{0\} \longrightarrow \mathbb{N}_0$ by $\delta(f(x)) = \deg f(x)$. Let $f(x), g(x) \in K[x] \setminus \{0\}$. Then $f(x)g(x) \neq 0$ and $\delta(f(x)g(x)) = \deg(f(x)g(x)) = \deg f(x) + \deg g(x) \geq \deg f(x) = \delta(f(x))$.

Let $f(x)$ and $g(x)$ be two polynomials in $K[x]$ such that $g(x) \neq 0$. Then the leading coefficient of $g(x)$ is nonzero and hence a unit in K. Then by Theorem 14.1.6, there exist $q(x), r(x) \in K[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$. Therefore, $K[x]$ is a Euclidean domain. □

Remark 14.1.13. Note that the quotient and the remainder of the division algorithm in the case of polynomial ring $K[x]$ over a field K are unique, by Theorem 14.1.6.

Corollary 14.1.14. *For a field K, $K[x]$ is a PID (and hence a UFD also).*

Proof. Follows from Theorems 14.1.12, 13.2.6 (and 13.1.21). □

Corollary 14.1.15. *Let K be a field and $f(x)$ be a polynomial in $K[x]$ with $\deg f(x) > 0$. Let $I = \langle f(x) \rangle$ be the principal ideal generated by $f(x)$. Then the following conditions are equivalent:*

(i) *$f(x)$ is an irreducible element in $K[x]$;*

(ii) *I is a maximal ideal of $K[x]$;*

(iii) *$K[x]/I$ is a field;*

(iv) *$K[x]/I$ is an integral domain;*

(v) *I is a prime ideal of $K[x]$;*

(vi) *$f(x)$ is a prime element in $K[x]$.*

Proof. Follows from Theorems 13.1.9, 12.3.10 and the Corollary 14.1.14 above. □

The following theorem is of great importance, as it proves that the converse[5] of Corollary 14.1.14 also holds.

Theorem 14.1.16. *Let R be a commutative ring with identity such that $R[x]$ is a PID. Then R is a field.*

[5] Only for the assertion outside parenthesis.

Proof. Let $a \in R \setminus \{0\}$ and let $I = (\{a, x\})$ be the ideal generated by a and x. Then $I = aR[x] + xR[x]$ as $R[x]$ is a commutative ring with identity. Since $R[x]$ is a PID, there exists $u \in R[x]$ such that $I = uR[x]$. Then $a = uv$ for some $v \in R[x]$. Now as $\deg a = 0$, we have $\deg u = \deg v = 0$. So $u \in R$. Also, $x \in I$ implies that $x = uf(x)$ for some $f(x) \in R[x]$. Again, as $\deg x = 1$ and $\deg u = 0$, it follows that $\deg f(x) = 1$. Thus $f(x) = b + cx$ for some $b, c \in R$. Then $x = u(b + cx)$, which implies that u is invertible (as $uc = 1$), i.e., a unit of R. Therefore $I = R[x]$ and hence $1 = ap(x) + xq(x)$ for some $p(x), q(x) \in R[x]$. Let $p(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n$. Then $1 = ac_0 + ac_1x + ac_2x^2 + \dots + ac_nx^n + xq(x)$. Hence $1 = ac_0$. This implies that a^{-1} exists in R. Therefore R is a field, as every nonzero element of R is a unit. □

Example 14.1.17. The above theorem shows at once that $\mathbb{Z}[x]$ is not a PID as $\mathbb{Z}$ is not a field. Similarly, we have for a field K, $K[x, y]$ (in general, $K[x_1, x_2, \dots, x_n]$ for $n > 1$) is not a PID. But we shall prove afterwards, using Gauss' theorem (cf. Theorem 14.1.27) that all these domains are UFD.

We shall now proceed to prove the Gauss' theorem which states that the polynomial ring over a UFD is also a UFD. We begin with the following definition.

Definition 14.1.18. Let R be a UFD and $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_nx^n \in R[x]$ be a polynomial with $a_n \neq 0$. Define the *content* of $f(x)$ by

$$c(f) = \gcd(a_0, a_1, a_2, \dots, a_n).$$

A polynomial $f(x) \in R[x] \setminus \{0\}$ is said to be *primitive* if $c(f) \sim 1$ (i.e., $c(f)$ is a unit).

In the polynomial ring $\mathbb{Z}[x]$, we know that 1 and -1 are the only units. Now $c(4+8x+2x^2) = \gcd(4, 8, 2) = 2$ shows that $4+8x+2x^2$ is not a primitive polynomial in $\mathbb{Z}[x]$, but $3+2x+7x^2+8x^3$ is a polynomial in $\mathbb{Z}[x]$ such that $c(3+2x+7x^2+8x^3) = \gcd(3, 2, 7, 8) = 1$, whence $3 + 2x + 7x^2 + 8x^3$ is a primitive polynomial in $\mathbb{Z}[x]$. However, we know that all the nonzero elements of $\mathbb{Q}$ are the units of $\mathbb{Q}[x]$, whence $4 + 8x + 2x^2$ is a primitive polynomial in $\mathbb{Q}[x]$.

Lemma 14.1.19. *Let R be a UFD. If $f(x) \in R[x]$, $f(x) \neq 0$, then $f(x) = c(f)g(x)$, where $g(x) \in R[x]$ is primitive.*

Proof. Follows immediately from the above definition. □

Now consider the polynomials $f(x) = 3 + 4x + 7x^2$ and $g(x) = 8 + 7x^2 + 9x^3$ in $\mathbb{Z}[x]$. Observe that $c(f) = \gcd(3, 4, 7) = 1$ and $c(g) = 1$. Hence both these polynomials are primitive. Now, $f(x)g(x) = (3 + 4x + 7x^2)(8 + 7x^2 + 9x^3) = 24 + 32x + 77x^2 + 55x^3 + 85x^4 + 63x^5$. It can be easily seen that $c(fg) = 1$. Hence $f(x)g(x)$ is also a primitive polynomial.

We prove this result in any polynomial ring $R[x]$, when R is a UFD.

Theorem 14.1.20. *Let R be a UFD and $f(x), g(x)$ be two primitive polynomials in $R[x]$. Then $f(x)g(x)$ is also a primitive polynomial. Moreover, for any $f(x), g(x) \in R[x] \setminus \{0\}$, $c(fg) \sim c(f)c(g)$.*

Proof. Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, $a_n \neq 0$ and $g(x) = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$, $b_m \neq 0$ be two primitive polynomials in $R[x]$. If $n = 0$, then $f(x) = a_0$ is a unit of R and $c(fg) \sim c(g) \sim 1$, as both $f(x)$ and $g(x)$ are primitive. So $f(x)g(x)$ is primitive. Similarly, the result holds for $m = 0$. Thus assume that $m, n \geq 1$.

Suppose, if possible, p is a prime factor of $c(fg)$. Now since $f(x)$ is primitive, p does not divide some coefficient a_i, $i \in \{0, 1, 2, \dots, n\}$. Let a_j be the first coefficient of $f(x)$ (i.e., j is the least value of i), which is not divisible by p. Similarly, let b_k be the first coefficient of $g(x)$, which is not divisible by p. In $f(x)g(x)$, the coefficient of x^{j+k} (say, c_{j+k}) is given by $c_{j+k} = (a_0b_{j+k} + a_1b_{j+k-1} + \dots + a_{j-1}b_{k+1}) + a_jb_k + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \dots + a_{j+k}b_0)$. Now, by our choice $p \mid b_r$ for all $r < k$ and $p \mid a_s$ for all $s < j$. Therefore, $p \mid (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + \dots + a_{j+k}b_0)$ and $p \mid (a_0b_{j+k} + a_1b_{j+k-1} + \dots + a_{j-2}b_{k+2} + a_{j-1}b_{k+1})$. Also since $p \mid c(fg)$, we have $p \mid c_{j+k}$. Thus $p \mid a_jb_k$. But this implies that $p \mid a_j$ or $p \mid b_k$, as p is prime, which is a contradiction. Hence there is no prime factor of $c(fg)$. In other words, $c(fg) \sim 1$, i.e., $f(x)g(x)$ is primitive.

The last part of the theorem follows from the above lemma. Let $f(x), g(x) \in R[x] \setminus \{0\}$. Then $f(x) = c(f)f_1(x)$ and $g(x) = c(g)g_1(x)$, where $f_1(x)$ and $g_1(x)$ are primitive. Thus $f(x)g(x) = c(f)c(g)f_1(x)g_1(x)$. By the above result, $f_1(x)g_1(x)$ is primitive and hence $c(fg) \sim c(f)c(g)$. □

Definition 14.1.21. Let R be a commutative ring with identity. Then a polynomial $f(x) \in R[x]$ is called *irreducible over* R, if $f(x)$ is an irreducible element in $R[x]$ (cf. Definition 13.1.3). A polynomial, which is neither zero nor a unit and which is not irreducible over R, is called *reducible over* R.

Example 14.1.22. $f(x) = 6 + 8x = 2(3 + 4x)$ shows that neither 2 nor $3 + 4x$ is a unit in $\mathbb{Z}[x]$. Hence $f(x)$ is not irreducible. Since $f(x)$ is a nonzero nonunit element in $\mathbb{Z}[x]$, it follows that, $f(x)$ is a reducible polynomial in $\mathbb{Z}[x]$. But the polynomial $3 + 4x$ is an irreducible polynomial in $\mathbb{Z}[x]$.

Remark 14.1.23. Note that every irreducible polynomial over a UFD R is primitive in $R[x]$, by Lemma 14.1.19.

Theorem 14.1.24. (Gauss' Lemma) *Let D be a UFD and E be the quotient field of D. Let $f(x) \in D[x]$ be a primitive polynomial of positive degree. Then $f(x)$ is irreducible in $D[x]$ if and only if $f(x)$ is irreducible in $E[x]$.*

Proof. Let $f(x)$ be an irreducible polynomial in $E[x]$. If $f(x) = g(x)h(x)$ in $D[x]$, then $g(x)$ and $h(x)$ cannot be both of positive degree, for then $f(x)$ would be reducible in $E[x]$ also. So let $\deg(g(x)) = 0$. Thus $g(x) \in D$. Since $f(x)$ is primitive in $D[x]$, it follows that $g(x)$ is a unit in D. Similarly, if $\deg(h(x)) = 0$, then $h(x)$ is a unit in D. So $f(x)$ is irreducible in $D[x]$.

Conversely, let $f(x)$ be irreducible in $D[x]$. Let if possible, $f(x)$ be reducible in $E[x]$. Then there exists nonzero nonunit elements $g(x)$ and $h(x)$ in $E[x]$ such that

$$f(x) = g(x)h(x)$$
$$= (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_n x^n)(\beta_0 + \beta_1 x + \beta_2 x^2 + \cdots + \beta_m x^m). \quad (14.1.3)$$

Since E is a field, an element $r(x) \in E[x] \setminus \{0\}$ is a unit if and only if $r(x)$ is of degree zero. Hence $g(x)$ and $h(x)$ are polynomials of positive degree in $E[x]$. Now for each $i = 0, 1, 2, \ldots, n$, $\alpha_i = a_i b_i^{-1}$ and for each $j = 0, 1, 2, \ldots, m$, $\beta_j = \bar{a}_j \bar{b}_j^{-1}$ for some $a_i, b_i, \bar{a}_j, \bar{b}_j \in D$.

Let $d = b_0 b_1 \ldots b_n \bar{b}_0 \bar{b}_1 \ldots \bar{b}_m \in D$. Multiplying both sides of (14.1.3) by d, we get

$$df(x) = \left(\sum_{i=0}^{n} c_i x^i\right)\left(\sum_{j=0}^{m} \bar{c}_j x^j\right) = u(x)v(x), \quad \text{(say)},$$

where $c_i = a_i b_0 b_1 \ldots b_{i-1} b_{i+1} \ldots b_n \in D$ and $\bar{c}_j = \bar{a}_j \bar{b}_0 \bar{b}_1 \ldots \bar{b}_{j-1} \bar{b}_{j+1} \ldots \bar{b}_m \in D$. Thus $u(x), v(x) \in D[x]$. So

$$df(x) = c(u)c(v)u_1(x)v_1(x),$$

where $u_1(x)$ and $v_1(x)$ are primitive polynomials in $D[x]$. Therefore, $d \sim c(u)c(v)$ as $f(x)$ is primitive. So $f(x) = \alpha u_1(x)v_1(x)$, where $\alpha \in D$ is a unit. But then $f(x)$ is reducible in $D[x]$ which is a contradiction. This completes the proof. □

Remark 14.1.25. Note that for each $f(x) \in E[x]$, there exist $a, b \in D$, $b \neq 0$ such that $f(x) = (ab^{-1})h(x)$, where $h(x) \in D[x]$ and $h(x)$ is primitive.

Lemma 14.1.26. *Let D be a UFD and E be the quotient field of D. If $f(x), g(x)$ be primitive polynomials in $D[x]$, then $f(x) \sim g(x)$ in $D[x]$ if and only if $f(x) \sim g(x)$ in $E[x]$.*

Proof. Suppose $f(x) \sim g(x)$ in $E[x]$. Then $g(x) = (ab^{-1})f(x)$ for some $a, b \in D$, $b \neq 0$. Then $bg(x) = af(x)$. Taking the contents of both sides we get $b \sim a$ (as $f(x)$ and $g(x)$ are primitive), i.e., $g(x) \sim f(x)$ in $D[x]$. The proof of the converse part is obvious. □

Theorem 14.1.27. (Gauss) *Let D be a UFD, then $D[x]$ is also a UFD.*

Proof. Let $f(x) \neq 0$ in $D[x]$. If $\deg(f(x)) = 0$, then $f(x) \in D$. Since D is a UFD, $f(x)$ has a unique factorization in D and hence in $D[x]$. So, let $\deg(f(x)) \geq 1$. Let E be the quotient field of D and we have $D \subseteq E$. Now $f(x) = c(f)g(x)$, where $g(x)$ is a primitive polynomial in $D[x] \subseteq E[x]$.

Since $g(x) \in E[x]$, $\deg(g(x)) \geq 1$ and $E[x]$ is a Euclidean domain by Theorem 14.1.12 and hence a UFD, it follows that

$$g(x) = q_1(x)q_2(x)\ldots q_m(x), \quad (14.1.4)$$

where each $q_i(x)$ is irreducible in $E[x]$ and is of a positive degree. Let $a_i, b_i \in D$, $(i = 1, 2, \ldots, m)$ be such that $q_i(x) = (a_i b_i^{-1})g_i(x)$, where $g_i(x) \in D[x]$ is a primitive polynomial. Then by (14.1.4),

$$b_1 b_2 \ldots b_m g(x) = a_1 a_2 \ldots a_m g_1(x)g_2(x)\ldots g_m(x).$$

Since the product of primitive polynomials is primitive by Theorem 14.1.20, it follows by taking contents of both sides that, $b_1 b_2 \ldots b_m \sim a_1 a_2 \ldots a_m$ in D, so that

$$g(x) = ug_1(x)g_2(x)\ldots g_m(x),$$

where u is a unit in D. Also since each $g_i(x)$ is irreducible in $E[x]$ and primitive in $D[x]$, it follows that $g_i(x)$, $i = 1, 2, \ldots, n$, are irreducible in $D[x]$, by Gauss' Lemma (Theorem 14.1.24). Thus,

$$f(x) = uc(f)g_1(x)g_2(x)\ldots g_m(x). \quad (14.1.5)$$

Now, if $c(f)$ is a unit in D, then $uc(f)g_1(x)$ is an irreducible element in $D[x]$. If $c(f)$ is not a unit, then by unique factorization property of D, there exist irreducible elements $d_1, d_2, \ldots, d_n$ in D such that $c(f) = d_1 d_2 \ldots d_n$ and hence $f(x) = \bar{d}_1 d_2 \ldots d_n g_1(x) g_2(x) \ldots g_m(x)$, where $\bar{d}_1 = d_1 u$. Now $d_1, d_2, \ldots, d_n$ are also irreducible elements in $D[x]$. Hence it follows that $f(x)$ can be expressed as a product of irreducible elements in $D[x]$.

We now show that any factorization of $f(x)$ in $D[x]$ is unique. To prove this, we first note that

$$f(x) = c(f)g_1(x)g_2(x)\ldots g_m(x),$$

where $g_i(x), i = 1, 2, \ldots, m$ are irreducible in $D[x]$. Now, any factorization of $f(x)$ in $D[x]$ must be of the form

$$f(x) = d_1 d_2 \ldots d_r g_1(x) g_2(x) \ldots g_m(x),$$

where either $c(f) = d_1 d_2 \ldots d_r = d$ is a unit or $d_1, d_2, \ldots, d_r$ are irreducible elements of D and $g_1(x), g_2(x), \ldots, g_m(x)$ are irreducible elements of $D[x]$.

Let

$$f(x) = c(f)g_1(x)g_2(x)\ldots g_m(x) = d_1 d_2 \ldots d_r g_1(x) g_2(x) \ldots g_m(x)$$

and

$$f(x) = c(f)h_1(x)h_2(x)\ldots h_s(x) = e_1 e_2 \ldots e_t h_1(x) h_2(x) \ldots h_s(x)$$

be two factorizations of $f(x)$ in $D[x]$. Then,

$$\begin{aligned} & g_1(x)g_2(x)\ldots g_m(x) \\ = \; & u h_1(x) h_2(x) \ldots h_s(x) \quad \text{where } u \text{ is a unit in } D \\ = \; & \bar{h}_1(x)\, \bar{h}_2(x) \ldots \bar{h}_s(x) \quad \text{where } \bar{h}_1(x) = u h_1(x) \\ & \text{and } \bar{h}_j(x) = h_j(x) \qquad \ldots (*) \end{aligned}$$

Since $g_i(x), i = 1, 2, \ldots, m$; $\bar{h}_1(x), h_j(x), j = 2, \ldots, s$ are irreducible and primitive in $D[x]$, therefore these polynomials are irreducible in $E[x]$. Now $E[x]$ is a UFD, hence from $(*)$, it follows that $m = t$ and there exists a permutation σ on $\{1, 2, \ldots, m\}$ such that $g_i(x) \sim h_{\sigma(i)}(x)$. Again, $c(f) \in D$ and D is a UFD, hence if $c(f)$ is not a unit, its factorization in D and hence in $D[x]$ is unique. Therefore the factorization of $f(x)$ in $D[x]$ is unique. Hence $D[x]$ is a UFD. □

Corollary 14.1.28. *Let D be a UFD, then $D[x_1, x_2, \ldots, x_n]$ is also a UFD. In particular, if K is a field, then $K[x_1, x_2, \ldots, x_n]$ is a UFD.*

Proof. Since $D[x_1, x_2, \ldots, x_n] \simeq D_{n-1}[x_n]$, where $D_{n-1} = D[x_1, x_2, \ldots, x_{n-1}]$, the result follows by induction on n from Gauss' theorem. □

The following diagram (Fig. 27) depicts the inter-relation among the various domains discussed so far.

$$ED \longrightarrow PID \longrightarrow UFD \longrightarrow FD \longrightarrow ID$$

Fig. 27

Till now we have discussed and established the inter-relationships as shown above, giving supporting examples in terms of various well-known structures. To put the state of affairs in a nutshell, we bring an end to this section with the following compact tabular representation, which substantiates the above diagram in terms of various examples.

ID	FD	UFD	PID	ED	Field
$\mathbb{Q}$	✓	✓	✓	✓	✓
$\mathbb{R}$	✓	✓	✓	✓	✓
$\mathbb{Z}$	✓	✓	✓	✓	×
$\mathbb{Q}[x]$	✓	✓	✓	✓	×
$\mathbb{R}[x]$	✓	✓	✓	✓	×
$\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$	✓	✓	✓	×	×
$\mathbb{Z}[x]$	✓	✓	×	×	×
$\mathbb{Z}[i\sqrt{5}]$	✓	×	×	×	×
R	×	×	×	×	×

where $R = \{a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Q}[x] \; ; \; a_0 \in \mathbb{Z}, n \in \mathbb{N}_0\}$ which is a subring of $\mathbb{Q}[x]$ with identity and hence an integral domain. But we have $x = 2\left(\frac{1}{2}x\right) = 2 \cdot 2\left(\frac{1}{4}x\right) = 2 \cdot 2 \cdot 2\left(\frac{1}{8}x\right)$ and so on. In general, one may verify that, x has no factorization interms of finite number of irreducible elements. Indeed, if $x = p(x)q(x)$ where $p(x), q(x)$ are nonzero nonunit elements of R then either $deg\, p(x) = 0$ and $deg\, q(x) = 1$ or the other way round. So, $x = a(bx + c)$, for some $a, c \in \mathbb{Z}, b \in \mathbb{Q}, a, b \neq 0$. Then $ac = 0$ and since R is an integral domain we have $c = 0$ i.e., $x = a(bx)$. Thus $ab = 1$. Since $a \in \mathbb{Z}$, let $a = n, b = \frac{1}{n}$. Then

$$x = n\left(\frac{1}{n}x\right) = n \cdot 2\left(\frac{1}{2n}x\right) = n \cdot 2 \cdot 2\left(\frac{1}{4n}x\right) = \ldots\ldots$$

where none of the terms within brackets is irreducible. Thus, x has no factorization, as claimed above. Hence R is an ID but not a FD.

Worked Out Exercises

◇ **Exercise 14.1.1.** If R is a commutative ring with identity, then show that $R[x]$ and R have the same characteristic.

Solution. We first note that R is a subring of $R[x]$ such that both have the same identity, 1. Now if R is of characteristic zero, then there is no such positive integer n so that $n1 = 0$. Then $R[x]$ is also of characteristic zero. Similarly, if $R[x]$ is of characteristic zero, then R also has the characteristic zero.

Again if R is of finite characteristic, then characteristic of R is a positive integer n, where n is the least positive integer such that $n1 = 0$. This implies that the characteristic of $R[x]$ is n, since 1 is also the identity of $R[x]$. Similar arguments prove the converse that if the characteristic of $R[x]$ is n, then R has the same characteristic.

◇ **Exercise 14.1.2.** Let $f(x) = x^5+[2]x^4+[2]x^3+[3]x^2+[4]x+[3]$ and $g(x) = x^3-[2]x^2+[3]x-[1]$ be two polynomials in $\mathbb{Z}_6[x]$. Find the polynomials $q(x), r(x) \in \mathbb{Z}_6[x]$ so that $f(x) = q(x)g(x) + r(x)$, where either $r(x) = [0]$ or $\deg r(x) < \deg g(x)$.

Solution. We follow the elementary division process: [6]

$$\begin{array}{r|l} & x^2+[4]x+[1] \\ \hline x^3-[2]x^2+[3]x-[1] & x^5+[2]x^4+[2]x^3+[3]x^2+[4]x+[3] \\ & x^5-[2]x^4+[3]x^3-x^2 \\ & -\quad+\quad-\quad+ \\ \hline & [4]x^4-x^3+[4]x^2+[4]x+[3] \\ & [4]x^4-[2]x^3-[4]x \\ & -\quad+\quad+ \\ \hline & x^3+[4]x^2+[2]x+[3] \\ & x^3-[2]x^2+[3]x-[1] \\ & -\quad+\quad-\quad+ \\ \hline & -x+[4] \end{array}$$

Thus the required quotient and remainder are given by

$$q(x) = x^2+[4]x+[1] \text{ and } r(x) = -x+[4].$$

One may easily verify that $f(x) = q(x)g(x) + r(x)$ with $\deg r(x) = 1 < 3 = \deg g(x)$.

[6] Care has to be taken that all the coefficients are in the ring $\mathbb{Z}_6$.

◇ **Exercise 14.1.3.** Find the gcd of the polynomials $f(x)$ and $g(x)$ in the polynomial ring $R[x]$, where

(i) $f(x) = x^4+3x^3-3x+1$, $g(x) = x^3+3x^2+x-2$ and $R = \mathbb{Q}$;

(ii) $f(x) = [2](x^5-x^4+x^3-x-[1])$, $g(x) = x^4-[2]x^2+[2]$ and $R = \mathbb{Z}_5$.

Solution. (i) We shall follow the Euclidean algorithm to find out the gcd:

$$\begin{array}{r|l} & x \\ \hline x^3+3x^2+x-2 & x^4+3x^3-3x+1 \\ & x^4+3x^3+x^2-2x \\ & -\quad-\quad-\quad+ \\ \hline & -x^2-x+1 \end{array}$$

Thus,

$$x^4+3x^3-3x+1 = (x^3+3x^2+x-2)(x) - (x^2+x-1),$$

i.e., $f(x) = xg(x) - (x^2+x-1)$. Again,

$$\begin{array}{r|l} & x+2 \\ \hline x^2+x-1 & x^3+3x^2+x-2 \\ & x^3+x^2-x \\ & -\quad-\quad+ \\ \hline & 2x^2+2x-2 \\ & 2x^2+2x-2 \\ & -\quad-\quad+ \\ \hline & 0 \end{array}$$

Therefore, $x^3+3x^2+x-2 = (x^2+x-1)(x+2)$ which implies that

$$\gcd(f(x), g(x)) = \gcd(x^4+3x^3-3x+1, x^3+3x^2+x-2) = x^2+x-1.$$

(ii) We have

$$\begin{array}{r|l} & [2]x-[2] \\ \hline x^4-[2]x^2+[2] & [2]x^5-[2]x^4+[2]x^3-[2]x-[2] \\ & [2]x^5-[4]x^3+[4]x \\ & -\quad+\quad- \\ \hline & -[2]x^4+x^3-x-[2] \\ & -[2]x^4+[4]x^2-[4] \\ & +\quad-\quad+ \\ \hline & x^3-[4]x^2-x+[2] \end{array}$$

$= x^3+\ x^2-$

$$
\begin{array}{r|l}
 & x-[1] \\
x^3+x^2-x+[2] & x^4 \quad -[2]x^2 \quad + [2] \\
 & x^4+x^3-x^2+[2]x \\
 & -x^3-x^2-[2]x+[2] \\
 & -x^3-x^2+x-[2] \\
 & -[3]x+[4] \\
 & = [2]x+[4] \\
 & = [2](x+[2])
\end{array}
$$

$$
\begin{array}{r|l}
 & x^2-x+[1] \\
x+[2] & x^3+x^2-x+[2] \\
 & x^3+[2]x^2 \\
 & -x^2-x+[2] \\
 & -x^2-[2]x \\
 & x+[2] \\
 & x+[2] \\
 & [0]
\end{array}
$$

Therefore,

$$
\begin{aligned}
f(x) &= [2](x^5-x^4+x^3-x-[1]) \\
&= (x^4-[2]x^2+[2])([2]x-[2])+x^3+x^2-x+[2], \\
x^4-[2]x^2+[2] &= (x^3+x^2-x+[2])(x-[1])+[2](x+[2]) \\
x^3+x^2-x+[2] &= (x+[2])(x^2-x+[1]).
\end{aligned}
$$

Hence $\gcd(f(x),g(x)) = \gcd\left([2](x^5-x^4+x^3-x-[1]), x^4-[2]x^2+[2]\right) = x+[2]$.

◊ **Exercise 14.1.4.** Let R be a commutative ring with identity and S be a subring of R which contains the identity. For $t \in R$, define $S[t] = \{f(t) \in R \mid f(x) \in S[x]\}$. Prove that $S[t]$ is a subring of R and there exists a unique homomorphism ϕ : $S[x] \longrightarrow S[t]$ such that $\phi(x) = t$ and $\phi(a) = a$ for all $a \in S$.

Solution. Certainly $0 \in S[t]$, as the zero-polynomial belongs to $S[x]$. Let $a, b \in S[t]$. Then there exist $f(x), g(x) \in S[x]$ such that $a = f(t)$ and $b = g(t)$. Let $h(x) = f(x) - g(x)$ and $k(x) = f(x)g(x)$. Then $h(x), k(x) \in S[x]$ and $h(t) = f(t) - g(t) = a - b$ and $k(t) = f(t)g(t) = ab$. So $a - b, ab \in S[t]$. This implies that $S[t]$ is a subring of R. Define $\phi : S[x] \longrightarrow S[t]$ by $\phi(f(x)) = f(t)$. Clearly, $\phi(x) = t$ and $\phi(a) = a$ for all $a \in S$.

Let $f(x), g(x) \in S[x]$. Let $p(x) = f(x) + g(x)$ and $q(x) = f(x)g(x)$. Then $\phi(p(x)) = p(t) = f(t) + g(t) = \phi(f(x)) + \phi(g(x))$ and $\phi(q(x)) = q(t) = f(t)g(t) = \phi(f(x))\phi(g(x))$. These imply that ϕ is a homomorphism such that $\phi(x) = t$ and $\phi(a) = a$ for all $a \in S$.

To show that ϕ is unique with this property, let $\psi : S[x] \longrightarrow S[t]$ a homomorphism with $\psi(x) = t$ and $\psi(a) = a$ for all $a \in S$. Let $f(x) = a_0 + a_1x + a_2x^2 \ldots + a_nx^n \in S[x]$. Then $\psi(f(x)) = \psi(a_0 + a_1x + a_2x^2 + \ldots + a_nx^n) = \psi(a_0) + \psi(a_1)\psi(x) + \psi(a_2)\{\psi(x)\}^2 + \ldots + \psi(a_n)\{\psi(x)\}^n = a_0 + a_1t + a_2t^2 + \ldots + a_nt^n = f(t) = \phi(f(x))$ since ψ is a homomorphism, $\psi(x) = t$ and $\psi(a) = a$ for all $a \in S$. Thus $\psi = \phi$ which proves the uniqueness of ϕ as required.

◊ **Exercise 14.1.5.** Let R be an integral domain and $f(x)$ be a nonzero polynomial in $R[x]$ of degree n. Then show that $f(x)$ has at most n roots in R (counted according to multiplicity).

Solution. We prove this result by induction on the degree n of $f(x)$. If $n = 0$, then $f(x)$ is a constant polynomial and so $f(x)$ has no roots in R. Therefore the result is true for $n = 0$. Suppose now the result is true for all polynomials of degree $k < n$, where $n \geq 1$. Let $f(x) \in R[x]$ and $\deg f(x) = n$. If $f(x)$ has no root in R, then we are done. Suppose $f(x)$ has a root a in R. Then by Corollary 14.1.9, $(x - a) \mid f(x)$. Let $f(x) = (x - a)^r g(x)$ where $g(x) \in R[x]$ and degree of $g(x) = n - r$. Then by induction hypothesis, $g(x)$ has at most $n - r$ roots in R. Let b be a root of $f(x)$ such that $b \neq a$. Then $0 = f(b) = (b - a)^r g(b)$ in R. Since R is an ID and $b - a \neq 0$, we find that $g(b) = 0$. Hence any root of $f(x)$ in R, different from a, is a root of $g(x)$. Therefore, $f(x)$ has at most $(n - r) + r = n$ roots. This completes the induction.

◊ **Exercise 14.1.6.** Let R be a commutative ring with identity. Show that $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a unit in $R[x]$ if and only if a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent elements of R.

Solution. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in R[x]$ where a_0 is a unit and $a_1, a_2, \ldots, a_n$ are nilpotent elements of R. Let $i \in \mathbb{N}$ be such that $1 \leqslant i \leqslant n$. Since a_i is nilpotent, there exists a positive integer k such that $a_i^k = 0 \in R$. Then $(a_ix^i)^k = a_i^k x^{ik} = 0 \in R[x]$. Thus a_ix^i is a nilpotent element in $R[x]$. Also, since sum of nilpotent elements is again a nilpotent element (cf. Theorem 11.1.21), we

have $f(x) - a_0$ is nilpotent in $R[x]$. Then, $a_0^{-1}f(x) = 1 + g(x)$ where $g(x)$ is a nilpotent element of $R[x]$. Let $g(x)^m = 0$ for some $m \in \mathbb{N}$. Now there exists a positive integer r such that $2^{r-1} < m \leq 2^r$. Then $g(x)^{2^r} = 0$. Now,

$$\begin{aligned} & \{a_0^{-1}f(x)\}(1-g(x))(1+g(x)^2)(1+g(x)^{2^2})\cdots(1+g(x)^{2^{r-1}}) \\ = & (1+g(x))(1-g(x))(1+g(x)^2)(1+g(x)^{2^2})\cdots(1+g(x)^{2^{r-1}}) \\ = & 1-g(x)^{2^r} = 1 \quad \text{as } g(x)^{2^r} = 0. \end{aligned}$$

Thus $f(x)h(x) = 1$ where $h(x) = a_0^{-1}(1-g(x))(1+g(x)^2)(1+g(x)^{2^2})\ldots(1+g(x)^{2^{r-1}})$. Therefore $f(x)$ is a unit in $R[x]$.

Conversely, let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a unit in $R[x]$. Then there exists $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in R[x]$ such that $f(x)g(x) = 1$. Thus $a_0b_0 = 1$ and hence a_0 is a unit in R. We use induction on $\deg(f(x))$ to prove that if a polynomial is a unit in $R[x]$, then all of its coefficients of the nonconstant terms are nilpotent. The result is obviously true for $n = 0$. Let us assume that it is also true for any unit polynomial of degree less than n. We prove the result for $f(x)$ described above, where $\deg f(x) = n$.

Now from $f(x)g(x) = 1$, we have

$$a_nb_m = 0, \tag{14.1.6}$$

$$a_nb_{m-1} + a_{n-1}b_m = 0, \tag{14.1.7}$$

$$a_nb_{m-2} + a_{n-1}b_{m-1} + a_{n-2}b_m = 0, \text{ etc.} \tag{14.1.8}$$

Multiplying both sides of (14.1.7) by a_n and using (14.1.6), we get $a_n^2b_{m-1} = 0$. Then multiplying both sides of (14.1.8) by a_n^2 and using (14.1.6) and (14.1.7), we get $a_n^3b_{m-2} = 0$. Proceeding in this way, we have $a_n^{m+1}b_0 = 0$ which implies that $a_n^{m+1} = 0$ as b_0 is a unit. Let $u(x) = a_nx^n$. Then $u(x)$ is nilpotent. Consider the polynomial $f_1(x) = f(x) - u(x) = f(x)(1 - u(x)g(x))$. Since $u(x)g(x)$ is nilpotent, arguing as in the previous case it can be shown that $1 - u(x)g(x)$ is a unit. Also since $f(x)$ is a unit, we have $f_1(x)$ is a unit. But $\deg f_1(x) = n - 1 < n$. Thus by induction hypothesis, $a_1, a_2, \ldots, a_{n-1}$ are nilpotent. We have already shown that a_n is nilpotent. Therefore a_i is nilpotent for all $i = 1, 2, \ldots, n$. This completes the induction and the proof.

Exercise 14.1.7. Let D be a Euclidean domain in which the Euclidean norm δ satisfies an additional condition that

$$\text{for any } a, b \in D, \ \delta(a+b) \leq \max\{\delta(a), \delta(b)\}.$$

Then either D is a field or $D \simeq K[x]$ where K is a field.

Solution. Let $K = \{a \in D \mid \delta(a) = \delta(1)\} \cup \{0\}$. Since for any $a, b \in K \setminus \{0\}$, either $a + b = 0 \in K$ or $a + b \neq 0$ and $\delta(a+b) \leq \max\{\delta(a), \delta(b)\} = \delta(1)$ and since $\delta(1)$ is the least element in the range of δ, we have $\delta(a+b) = \delta(1)$, which again implies $a + b \in K$. If $a = 0$, then $a + b = b \in K$. Similarly, if $b = 0$, then $a + b = a \in K$. Also by Remark 13.2.2, we have $\delta(-a) = \delta(a)$ for all $a \in K \setminus \{0\}$ and the set $K \setminus \{0\}$ is the group of units of D. Thus K is a subfield of the domain D. If $D = K$, we have nothing to prove.

So suppose $D \neq K$. Let $T = \{\delta(a) \mid a \in D \setminus K\}$. Then T is a nonvoid subset of $\mathbb{N}$ contained in $T_1 = \{n \in \mathbb{N} \mid n > \delta(1)\}$. Let $c \in D \setminus K$ be such that $\delta(c) = m > \delta(1)$ is the least element in T. Now for any $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in K[x]$, define $f(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$. Clearly, $K[c] = \{f(c) \mid f(x) \in K[x]\}$ is a subring of D as $K \subseteq D$ and $c \in D$. We show, by induction, that $D = K[c]$.

Let $d \in D$. If $\delta(d) = \delta(1)$, then $d \in K \subseteq K[c]$. Assume that for each $d \in D$, $\delta(d) < k$ implies that $d \in K[c]$. Let $d \in D$ be such that $\delta(d) = k$. Since D is a Euclidean domain, $d = qc + r$ for some $q, r \in D$ where either $r = 0$ or $\delta(r) < \delta(c) = m$. Now if $r \neq 0$, then $\delta(r) < m$, which implies that $\delta(r) = \delta(1)$. Now as c is not a unit in D, we have $\delta(q) < \delta(qc)$ (cf. Worked Out Exercise 13.2.2). Thus, in this case, $\delta(q) < \delta(qc) \leq \delta(d - r) \leq \max\{\delta(d), \delta(-r)\} = \max\{k, \delta(r)\} = \max\{k, \delta(1)\} = k$. Also if $r = 0$, then $\delta(q) < \delta(qc) = \delta(d) = k$. Therefore by induction hypothesis, $q \in K[c]$ which implies that $d = qc + r \in K[c]$ as in either case $r \in K$. Thus $D \subseteq K[c]$ and hence $D = K[c]$.

Now it is easy to verify that the map $\phi : K[x] \longrightarrow K[c]$ defined by $\phi(f(x)) = f(c)$ is an epimorphism.[7] We show that ϕ is an isomorphism, indeed. For this, we prove that if $f(c) = 0$ for some $f(x) \in K[x]$, then $f(x)$ is identically zero. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with $a_n \neq 0$. Let us prove by induction that $f(c) \neq 0$ for any n. If $n = 0$, then $f(x) = a_0 \neq 0$ and so $f(c) = a_0 \neq 0$. Suppose the result is true for any $m < n$. Let $\deg f(x) = n$. Now if $f(c) = 0$, then

$$c^n = -(a_n^{-1}a_0 + a_n^{-1}a_1c + a_n^{-1}a_2c^2 + \cdots + a_n^{-1}a_{n-1}c^{n-1}).$$

[7] Certainly, we mean a ring epimorphism.

So by Worked Out Exercise 13.2.2,

$$\begin{aligned}\delta(c^{n-1}) &< \delta(c^n)\\ &\le \max\{\delta(a_n^{-1}a_0), \delta(a_n^{-1}a_1c), \delta(a_n^{-1}a_2c^2), \ldots, \delta(a_n^{-1}a_{n-1}c^{n-1})\}\\ &= \max\{\delta(1), \delta(c), \delta(c^2), \ldots, \delta(c^{n-1})\}\\ &= \delta(c^{n-1}),\end{aligned}$$

which is a contradiction. Thus $f(c) \neq 0$. This completes the induction and hence we get that if $f(c) = 0$, then $f(x) = 0$ in $K[x]$. This implies that ϕ is an isomorphism, i.e., $D = K[c] \simeq K[x]$, as required.

Exercises

1. In $\mathbb{Z}_6[x]$, find $f(x)+g(x), f(x)g(x), \deg f(x), \deg g(x), \deg(f(x)+g(x))$ and $\deg(f(x)g(x))$ where $f(x) = [2] + [3]x + x^2 + [2]x^5$, $g(x) = [1] + [2]x^2 + [5]x^3 + [3]x^4$.
2. In $\mathbb{Z}_7[x]$, let $f(x) = [2] + [3]x + x^2 + [2]x^5$, $g(x) = [1] + [2]x^2 + [5]x^3 + [3]x^4$. Find $f(x) + g(x), f(x)g(x), \deg f(x), \deg g(x), \deg(f(x) + g(x))$ and $\deg(f(x)g(x))$.
3. Let $f(x) = x^2 + x + [4] \in \mathbb{Z}_{10}[x]$. Show that $[7]$ is a root of $f(x)$.
4. In $\mathbb{Z}_5[x]$, express the polynomial $x^4 + [4]$ as a product of linear factors.
5. In $\mathbb{Z}_7[x]$, factorize $f(x) = x^3 + [1]$ into linear factors.
6. Find all the roots of the polynomial $x^5 - [3]x^3 + [4]x^2 + x + [2] \in \mathbb{Z}_7[x]$ which lie in $\mathbb{Z}_7$.
7. Let R be the ring $\mathbb{Z} \times \mathbb{Z}$. Solve the polynomial equation: $(1,1)x^2 - (5,14)x + (6,33) = (0,0)$ over R. Show that the linear equation, $(5,0)x + (20,0) = (0,0)$ has infinitely many roots in R.
8. Let $f(x) = [3]x^4 + x^3 + [2]x^2 + [4]$, $g(x) = x^2 - [4]x + [2]$ in $\mathbb{Z}_5[x]$. Find the quotient and remainder upon dividing $f(x)$ by $g(x)$.
9. Let $f(x) = 12x^7 - 44x^6 - 49x^5 + 54x^4 + 68x^3 - 5x^2 - 34x - 18$ and $g(x) = 2x^4 - 9x^3 + 7x + 1$ be two polynomials in $\mathbb{Q}[x]$. Find the polynomials $q(x), r(x) \in \mathbb{Q}[x]$ so that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
10. Let $f(x) = [2]x^6 - x^5 + [3]x^4 + [3]x^3 - [5]x^2 + [4]$ and $g(x) = [2]x^4 - [3]x^2 + [5]x + [1]$ be two polynomials in $\mathbb{Z}_7[x]$. Find the polynomials $q(x), r(x) \in \mathbb{Z}_7[x]$ so that $f(x) = q(x)g(x) + r(x)$ where either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
11. Find the gcd of the polynomials $f(x)$ and $g(x)$ in the polynomial ring $R[x]$, where
    (i) $f(x) = 2x^5 + 3x^4 + 9x^3 + x^2 + 13x + 20$; $g(x) = 3x^4 - x^3 + 12x^2 - 13x + 55$ and $R = \mathbb{Q}$.
    (ii) $f(x) = x^3 + x + [1]$, $g(x) = x^3 - x^2 - [1]$ and $R = \mathbb{Z}_3$;
    (iii) $f(x) = x^5 - x^4 + [3]x^3 - [3]x^2 + [3]x + [6]$, $g(x) = [3]x^4 - [3]x^2 - [5]x + [8]$ and $R = \mathbb{Z}_{13}$.

12. Find all polynomials of degree 2 in $\mathbb{Z}_2[x]$.
13. Let K be an infinite field and $f(x) \in K[x]$. If $f(x)$ has infinite roots in K, then prove that $f(x)$ is the zero polynomial.
14. Let R be an integral domain. Show that an element u is a unit in $R[x]$ if and only if u is a unit in R.
15. Let K be a field and $p(x) \in K[x]$. Let P be the principal ideal generated by $p(x)$. Prove that $K[x]/P$ is an integral domain if and only if $K[x]/P$ is a field.
16. Let K be a field. Suppose $\phi : K[x] \longrightarrow K[x]$ be an automorphism such that $\phi(u) = u$ for all $u \in K$. Prove that $\phi(x) = ax + b$ for some $a, b \in K$.
17. Let R be a UFD and $f(x) \in R[x]$ be a primitive polynomial of degree ≥ 1. Prove that every positive degree factor of $f(x)$ is also primitive.
18. Let K be a field and $f(x) \in K[x]$ with $\deg f(x) = n > 0$. Let $I = (f(x))$, the principal ideal generated by $f(x)$. Show that

$$K[x]/I = \{g(x) + I \mid g(x) \in K[x],\ \text{either } g(x) = 0 \text{ or } \deg g(x) < n\}.$$

19. Let R be a commutative ring with identity. Prove that $R[x]/(x) \simeq R$, where (x) is the principal ideal generated by x.
20. Construct a polynomial ring $R[x]$ for any commutative ring R (possibly without identity). Show that R is a subring of $R[x]$ and if I is any ideal of R, then $I[x]$ is also an ideal of $R[x]$.
21. Prove that $\mathbb{Z}_4[x]$ has infinitely many units and infinitely many nilpotent elements.
22. Factorize $x^3 - 1$ as a product of irreducible polynomials in $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ and in $\mathbb{Z}_5[x], \mathbb{Z}_6[x]$.
23. Give an example of a ring R with identity and a maximal ideal I of R such that $I[x]$ is not a maximal ideal in $R[x]$.
24. Let R be a commutative ring with identity. If I is a prime ideal of R, show that $I[x]$ is a prime ideal of $R[x]$.
25. Is it true that $\mathbb{Z}[x] \simeq \mathbb{Z}$? Does there exist a commutative ring R such that $R[x] \simeq \mathbb{Z}$?
26. Find the correct answer in the following:
    (a) The number of zeros of $[2]x + [1]$ in $\mathbb{Z}_4[x]$ is
    (i) 1 (ii) 2 (iii) 0 (iv) 4
    (b) The number of zeros of $x^2 + [3]x + [2]$ in $\mathbb{Z}_6[x]$ is
    (i) 4 (ii) 2 (iii) 0 (iv) 1
    (c) The number of idempotent elements in $\mathbb{Z}_4[x]$ is
    (i) 1 (ii) 2 (iii) Infinite (iv) 4
    (d) The number of units in $\mathbb{Z}_5[x]$ is
    (i) 1 (ii) 2 (iii) 4 (iv) Infinite
    (e) If $f(x) = x^3 + [3]x + [2] \in \mathbb{Z}_5[x]$ then the number of roots of $f(x)$ in $\mathbb{Z}_5$ is
    (i) 0 (ii) 1 (iii) 3 (iv) 2

27. Find whether the following statements are true or false. Justify your answer giving counter examples whenever necessary.
   (a) The characteristic of $\mathbb{Z}_2[x]$ is 2.
   (b) $\mathbb{Z}_2[x]$ is a finite field.
   (c) $K[x]$ may be a field for some field K.
   (d) $x^2 - 2$ is irreducible in $\mathbb{Z}[x]$.
   (e) The ideal (x) in $\mathbb{Q}[x]$ is maximal.
   (f) $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ but not so in $\mathbb{R}[x]$.
   (g) In $\mathbb{Z}_6[x]$, $[2]x + [3]$ is an associate of $[3]x + [2]$.
   (h) In $\mathbb{Z}_5[x]$, $[3]x^2 + [4]x + [3] = ([4]x + 1)([2]x + [3])$.
   (i) $6 + 2x + 8x^2 + 12x^3$ is a primitive polynomial in $\mathbb{Q}[x]$.
   (j) $x^2 + 2x + 1$ is primitive but not irreducible in $\mathbb{Z}[x]$.
   (k) $2x + 4$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$.

28. † Find two polynomials $f, g \in \mathbb{Z}[x]$ such that $\gcd(f, g) = 1$ but there exist no pair of polynomials $h, k \in \mathbb{Z}[x]$ so that $fh + gk = 1$.

14.2 Irreducibility of Polynomials

It is clear from Gauss' theorem discussed in the last section, that every polynomial ring over a unique factorization domain is again a unique factorization domain. This implies that every polynomial over a UFD R has a unique factorization in $R[x]$ in terms of its irreducible elements, i.e., irreducible polynomials. Though the existence of such a factorization is ensured by Gauss' Theorem, but obtaining that explicitly, often becomes a very hard problem. There is no general method known for obtaining this factorization, not even for deciding whether a polynomial is irreducible or not. *It is still an open problem to get a (general) necessary and sufficient criterion for irreducibility of a polynomial (even over the field of rational numbers).* However we have some sufficient conditions for this. The Eisenstein's criterion, given below, is the most famous one.

Theorem 14.2.1. (Eisenstein's criterion) *Let D be a UFD and E be the quotient field of D. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a nonconstant polynomial in $D[x]$. Suppose there exists a prime $p \in D$ such that*

(i) $p \mid a_i$, $i = 0, 1, 2, \ldots, n-1$
(ii) $p \nmid a_n$
(iii) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible in $E[x]$. Moreover, if $f(x)$ is primitive, then $f(x)$ is irreducible in $D[x]$.

Proof. First, we note that there exists a primitive polynomial $g(x) \in D[x]$ such that $f(x) = c(f)g(x)$. Now, either $c(f) \sim 1$ or $c(f) \nsim 1$. Suppose $c(f) \sim 1$. Then $f(x) \sim g(x)$. Hence $f(x)$ is a primitive polynomial. In this case, we show that $f(x)$ is irreducible in $D[x]$. Suppose $f(x)$ is not irreducible. Now $f(x)$ is a nonconstant polynomial. Hence there exist two nonzero nonunit polynomials $h_1(x) = c_0 + c_1x + \ldots + c_mx^m$ and $h_2(x) = d_0 + d_1x + \ldots + d_rx^r$ in $D[x]$ such that $f(x) = h_1(x)h_2(x)$. Then $n = r + m$. If $h_1(x) = c_0$ then $c_0 \neq 0$, nonunit and $f(x) = c_0h_2(x)$ implies that $f(x)$ is not primitive. Hence $m > 0$. Similarly $r > 0$. Hence $0 < r < n$ and $0 < m < n$. Now $f(x) = h_1(x)h_2(x)$ implies that $a_0 = c_0d_0$. Since $p \mid a_0$, $p \mid c_0d_0$. Hence either $p \mid c_0$ or $p \mid d_0$. Again, $p^2 \nmid a_0$. Hence p cannot divide both of c_0 and d_0. So (without any loss of generality) assume that p divides c_0 and p does not divide d_0. Again $a_n = c_md_r$ and $p \nmid a_n$. Hence $p \nmid c_m$ and $p \nmid d_r$. So, we find that $p \mid c_0$ and $p \nmid c_m$. Hence, there exists a positive integer $i \leq m$ such that $p \mid c_0, \ldots, p \mid c_{i-1}$ but $p \nmid c_i$. Considering the coefficient of x^i in $f(x)$ and in $h_1(x)h_2(x)$, we find that

$$a_i = c_id_0 + c_{i-1}d_1 + \ldots + c_0d_i \tag{14.2.1}$$

where $c_{m+1} = c_{m+2} = \ldots = 0$ and $d_{r+1} = d_{r+2} = \ldots = 0$ in (14.2.1). Now as $p \mid c_0, p \mid c_1, \ldots, p \mid c_{i-1}$, we find that $p \mid a_i - c_id_0$. Since $i \leq m < n$, it follows from assumption (i) that $p \mid a_i$. Hence $p \mid c_id_0$. But $p \nmid c_i$ and $p \nmid d_0$ which is not possible as p is a prime integer. Hence $f(x)$ is irreducible in $D[x]$. Since $f(x)$ is also primitive, so from Gauss' lemma, $f(x)$ is irreducible in $E[x]$.

We now consider the case when $c(f)$ is not a unit in $D[x]$. Let $c(f) = d$. Then $f(x) = dg(x)$ where $g(x)$ is a primitive polynomial in $D[x]$. Let $g(x) = t_0 + t_1x + \ldots + t_nx^n$. Then $a_i = dt_i$, $i = 0, 1, \ldots, n$. Since $p \nmid a_n$, $p \nmid d$. Hence for the polynomial $g(x)$, we find $p \mid t_i$, $i = 0, 1, \ldots, n-1$, $p \nmid t_n$ and $p^2 \nmid t_0$. Hence from the above case, it follows that $g(x)$ is irreducible in $E[x]$. Since d is a unit in $E[x]$, we find that $f(x) \sim g(x)$ in $E[x]$. Therefore $f(x)$ is irreducible in $E[x]$. □

Corollary 14.2.2. *Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a nonconstant polynomial in $\mathbb{Z}[x]$. Suppose there exists a prime p such that*

(i) $p \mid a_i$, $i = 0, 1, 2, \ldots, n-1$
(ii) $p \nmid a_n$
(iii) $p^2 \nmid a_0$.

Then $f(x)$ is irreducible over $\mathbb{Q}$. Moreover, if $f(x)$ is primitive, then $f(x)$ is irreducible over $\mathbb{Z}$.

Proof. Follows from the above theorem and fact that $\mathbb{Z}$ is a UFD and $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$. □

Example 14.2.3. Let $f(x) = 5x^4 + 4x^3 - 6x^2 - 14x + 2 \in \mathbb{Z}[x]$. Then $2 \nmid 5$, $2 \mid 4$, $2 \mid (-6)$, $2 \mid (-14)$, $2 \mid 2$ but $2^2 \nmid 2$. Thus $f(x)$ is an irreducible polynomial over $\mathbb{Q}$, by Eisenstein's criterion. Also since $f(x)$ is primitive, it is irreducible over $\mathbb{Z}$.

Example 14.2.4. Let us consider the polynomial $f(x) = 1 + x + x^2 + x^3 + \cdots + x^{p-1} \in \mathbb{Z}[x]$, where p is a prime number. This polynomial is called a *cyclotomic polynomial*. Clearly f is primitive. Now consider the polynomial $f(x+1)$. Since $f(x) = \frac{x^p - 1}{x-1}$, we have

$$\begin{aligned} f(x+1) &= \frac{(x+1)^p - 1}{(x+1) - 1} \\ &= \frac{x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{i}x^{p-i} + \cdots + px}{x} \\ &= x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{i}x^{p-i-1} + \cdots + p, \end{aligned}$$

which is clearly irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Now it is easy to understand that if there is a nontrivial factorization of $f(x)$, say, $f(x) = g(x)h(x)$, then there is also a nontrivial factorization of $f(x+1)$, namely, $f(x+1) = g(x+1)h(x+1)$. Therefore $f(x)$ is irreducible over $\mathbb{Q}$ and hence over $\mathbb{Z}$, as $f(x)$ is primitive in $\mathbb{Z}[x]$.

In the following, we shall describe some other conditions for irreducibility of polynomials.

Theorem 14.2.5. *Let F be a field and $f(x) \in F[x]$ with $\deg f(x) = 2$ or 3. Then $f(x)$ is irreducible over F if and only if $f(x)$ has no root in F.*

Proof. Suppose $\deg f(x) = 3$ and $f(x)$ is irreducible. If $f(x)$ has a root in F, say a, then $x - a$ divides $f(x)$ in $F[x]$ and so $f(x)$ is reducible over F.

Conversely, suppose $f(x)$ has no roots in F. Assume that $f(x)$ is reducible. Then $f(x) = g(x)h(x)$ for some $g(x), h(x) \in F[x]$, $\deg g(x) \geq 1$ and degree $h(x) \geq 1$. Now if $\deg f(x) = \deg(g(x)h(x)) = 3$, then either $\deg g(x) = 1$ and $\deg h(x) = 2$ or the other way round. To be concrete, let $\deg g(x) = 1$ and $\deg h(x) = 2$. Then $g(x) = ax + b$ for some $a, b \in F$, $a \neq 0$. Now $-a^{-1}b \in F$ and $g(-a^{-1}b) = 0$. Thus, $-a^{-1}b$ is a root of $g(x)$ and hence $-a^{-1}b$ is a root of $f(x)$ in F. This is a contradiction to

our assumption that $f(x)$ has no roots in F. Hence, $f(x)$ is irreducible over F. A similar argument can be used for the case when $\deg f(x) = 2$. □

By virtue of the above theorem, we can find some irreducible polynomials. For example, $x^2 + 1$, $x^2 + 5$ have no roots in $\mathbb{R}$. Hence these are irreducible polynomials, whereas $x^3 + 1$ has a root -1 in $\mathbb{R}$, whence it is not an irreducible polynomial; rather $x^3 + 1 = (x+1)(x^2 - x + 1)$ shows that $x^3 + 1$ is reducible in $\mathbb{R}[x]$. Again consider the field $\mathbb{Z}_3$. $x^3 + [2]x + [2]$ is a polynomial in $\mathbb{Z}_3[x]$. Now none of the elements $[0]$, $[1]$ and $[2]$ are roots of this polynomial. Hence $x^3 + [2]x + [2]$ is an irreducible polynomial in $\mathbb{Z}_3[x]$.

The following theorem provides a very useful criterion to determine rational roots of a polynomial in $\mathbb{Z}[x]$.

Theorem 14.2.6. *Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in \mathbb{Z}[x]$ with $a_0, a_n \neq 0$. If $\frac{p}{q} \in \mathbb{Q}$ is a root of $f(x)$ (where p and q are relatively prime integers and $q > 0$), then $p \mid a_0$ and $q \mid a_n$.*

Proof. We have $f(\frac{p}{q}) = 0$ and so $a_0 + a_1(\frac{p}{q}) + a_2(\frac{p}{q})^2 + \cdots + a_n(\frac{p}{q})^n = 0$ which implies that

$$a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + \cdots + a_{n-1}p^{n-1}q + a_np^n = 0.$$

Thus we have $p \mid a_0q^n$ and $q \mid a_np^n$, since all other terms are divisible by p and q. But p and q are relatively prime. So $p \mid a_0$ and $q \mid a_n$, as required. □

Example 14.2.7. (i) Consider the polynomial $f(x) = 9x^3 - 7x^2 + 11x + 5$ over $\mathbb{Z}$. Here $a_0 = 5$ and $a_3 = 9$. Now the only factors of 5 are ± 1 and ± 5, whereas factors of 9 are $\pm 1, \pm 3, \pm 9$. Thus by the above theorem, possible rational roots of $f(x)$ are $\pm 1, \pm 5, \pm\frac{1}{3}, \pm\frac{5}{3}, \pm\frac{1}{9}, \pm\frac{5}{9}$. But one may easily verify that none of them is a root of $f(x)$ and hence by Theorem 14.2.5, $f(x)$ is irreducible over $\mathbb{Q}$ as well as over $\mathbb{Z}$, since $f(x)$ is primitive.

(ii) Next consider the polynomial $g(x) = x^3 - 9x^2 + 15x - 2$. According to the previous theorem, the only possible rational roots of $g(x)$ are ± 2 and we see that $g(2) = 0$. Therefore $g(x)$ is not irreducible over $\mathbb{Q}$.

Finally, we note that, in order to determine the irreducibility of a polynomial in $\mathbb{Z}[x]$, it is sometimes useful to consider the corresponding polynomial in $\mathbb{Z}_p[x]$ for

Theorem 14.2.8. *Let $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $n > 1$. If there exists a prime number p such that*

(i) $p \nmid a_n$ and

(ii) $\bar{f}(x) = [a_0] + [a_1]x + \dots + [a_n]x^n$ is irreducible in $\mathbb{Z}_p[x]$,

then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Proof. If possible, let $f(x)$ be reducible in $\mathbb{Q}[x]$. Now if $f(x)$ is irreducible in $\mathbb{Z}[x]$ then it is primitive by Remark 14.1.23 and hence it is also irreducible in $\mathbb{Q}[x]$ by Gauss' lemma (cf. Theorem 14.1.24). Thus, $f(x)$ is reducible in $\mathbb{Z}[x]$ and $f(x) = g(x)h(x)$ where $g(x) = b_0 + b_1x + \dots + b_mx^m$ and $h(x) = c_0 + c_1x + \dots + c_tx^t$ belong to $\mathbb{Z}[x]$ such that $\deg g(x) = m$, $\deg h(x) = t$ and $1 < m < n$, $1 < t < n$.

Now in $\mathbb{Z}_p[x]$, $[a_0] + [a_1]x + \dots + [a_n]x^n = ([b_0] + [b_1]x + \dots + [b_m]x^m)([c_0] + [c_1]x + \dots + [c_t]x^t)$. Hence $[a_n] = [b_m][c_t]$. Now $p \nmid a_n$. Hence $[a_n] \neq [0]$. Then $[b_m] \neq [0]$ and $[c_t] \neq [0]$. Therefore, $\bar{f}(x)$ is reducible in $\mathbb{Z}_p[x]$, which is a contradiction. Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$. ☐

Example 14.2.9. Let $f(x) = 13x^3 - 8x^2 + 11x - 3$. As a polynomial of $\mathbb{Z}_2[x]$, $\bar{f}(x) = x^3 + x + [1]$ which is irreducible over $\mathbb{Z}_2$ as $\bar{f}([0]) = \bar{f}([1]) = [1] \neq [0]$ (by Theorem 14.2.5). Also $2 \nmid 13$. Thus by the above theorem, $f(x)$ is irreducible over $\mathbb{Q}$.

Worked Out Exercises

◊ **Exercise 14.2.1.** Let F be a field. Show that every polynomial of degree 1 is an irreducible polynomial in $F[x]$.

Solution. Since $\deg f(x) = 1$, $f(x)$ is nonzero and nonunit. Suppose $f(x) = g(x)h(x)$, where $g(x), h(x) \in K[x]$. Clearly, $g(x), h(x)$ are nonzero polynomials. Now $1 = \deg f(x) = \deg g(x) + \deg h(x)$. Hence either $\deg g(x) = 1$ and $\deg h(x) = 0$ or, $\deg g(x) = 0$ and $\deg h(x) = 1$. Hence either $g(x) \in F \setminus \{0\}$ or $h(x) \in F \setminus \{0\}$. This implies that either $g(x)$ is a unit or $h(x)$ is a unit. Hence $f(x)$ is irreducible.

◊ **Exercise 14.2.2.** Let F be a field and $f(x) \in F[x]$ with $\deg f(x) \geq 2$. If $f(x)$ is irreducible in $F[x]$, then show that $f(x)$ has no root in F. Show that the converse of this result is not always true.

Solution. Let a be a root of $f(x)$ in F. Then by Remainder theorem, $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$. Now $\deg f(x) \geq 2$. Hence $\deg g(x) \geq 1$. Therefore $f(x)$ is not irreducible in $F[x]$. Hence if $f(x)$ is irreducible in $F[x]$, then $f(x)$ has no root in F.

Now consider the polynomial $f(x) = (x^2 + 1)(x^2 + 2)$ in $\mathbb{Q}[x]$. This polynomial has no root in $\mathbb{Q}$. But $f(x)$ is reducible in $\mathbb{Q}[x]$.

◊ **Exercise 14.2.3.** Show that $f(x) = x^3 + [2]x + [4]$ is irreducible in $\mathbb{Z}_5[x]$.

Solution. $f([0]) = [4]$; $f([1]) = [7] = [2]$, $f([2]) = [3] + [4] + [4] = [1]$, $f([3]) = [2] + [1] + [4] = [2]$, $f([4]) = [4] + [3] + [4] = [1]$. Hence $f(x)$ has no roots in $\mathbb{Z}_5$. Thus, $f(x)$ is irreducible in $\mathbb{Z}_5[x]$.

◊ **Exercise 14.2.4.** Let R be a UFD and $f(x) \in R[x]$. Show that $f(x)$ is irreducible over R if and only if $f(x + a)$ is irreducible over R for any $a \in R$.

Solution. Let $f(x)$ be irreducible over R. If $f(x + a)$ is not irreducible, then $f(x + a) = g(x)h(x)$, where $g(x)$ and $h(x)$ are nonzero and nonunit elements in $R[x]$. Thus $f(x) = g(x - a)h(x - a)$. Clearly, $g(x - a)$ and $h(x - a)$ are not zero (i.e., not the zero polynomial as $g(x)$, $h(x)$ are not so). Also, only units of $R[x]$ are units of R, as R is an integral domain. Now if $g(x - a)$ is a unit, then it is a constant polynomial and hence it is equal to $g(x)$ which implies that $g(x)$ is also a unit. Therefore $g(x - a)$ is not a unit. Similarly, $h(x - a)$ is not a unit. But then $f(x)$ is not irreducible, which is a contradiction. Thus $f(x + a)$ is also irreducible. In an exactly similar way, one can prove the converse that if $f(x + a)$ is irreducible, then $f(x)$ is also so.

◊ **Exercise 14.2.5.** Show that the following polynomials are irreducible:

(i) $2x^4 + 6x^3 - 9x^2 + 15$ over $\mathbb{Z}$;

(ii) $x^3 + 2x^2 + 3$ over $\mathbb{Q}$;

(iii) $x^5 + x^2 + [1]$ over $\mathbb{Z}_2$;

(iv) $x^3 - [9]$ over $\mathbb{Z}_{31}$.

Solution. (i) Let $f(x) = 2x^4 + 6x^3 - 9x^2 + 15$. Now 3 is prime in $\mathbb{Z}$ and $3 \nmid 2$, $3 \mid 6$, $3 \mid 9$, $3 \mid 15$ but $3^2 = 9 \nmid 15$. Thus following Eisenstein's criterion, we have $f(x)$ is irreducible over $\mathbb{Q}$, the quotient field of $\mathbb{Z}$. Moreover $f(x)$ is primitive, as $\gcd(2, 6, 9, 15) = 1$. Therefore $f(x)$ is irreducible over $\mathbb{Z}$.

(ii) Let $f(x) = x^3 + 2x^2 + 3$. Since $\deg f(x) = 3$, we have if $f(x)$ is not irreducible (over $\mathbb{Q}$), then $f(x)$ must have a linear factor, i.e., $f(x)$ has a root over $\mathbb{Q}$. Now by Theorem 14.2.6, the possible roots of $f(x)$ are $\frac{p}{q}$, $(p, q \in \mathbb{Z}, q \neq 0)$, where $p \mid 3$, and $q \mid 1$. The only possibilities are ± 3. But $f(3) = 48 \neq 0$ and $f(-3) = -6 \neq 0$. Therefore $f(x)$ has no linear factor and hence $f(x)$ is irreducible over $\mathbb{Q}$.

(iii) Let $f(x) = x^5 + x^2 + [1] \in \mathbb{Z}_2[x]$. First we note that $f(x)$ has no linear factor as $f([0]) = [1] = f([1])$. Thus if $f(x)$ is not irreducible, then $f(x)$ must have an irreducible quadratic factor. Now there are four quadratic polynomials in $\mathbb{Z}_2[x]$, namely x^2, $x^2 + [1]$, $x^2 + x$, $x^2 + x + [1]$ and among them, the only[8] irreducible one is $x^2 + x + [1]$.

Let $f(x) = (x^2 + x + [1])(x^3 + ax^2 + bx + c)$ where $a, b, c \in \mathbb{Z}_2$. Then we have $[1] + a = [0]$, $[1] + a + b = [0]$, $a + b + c = [1]$, $b + c = [0]$, $c = [1]$. The first two equalities imply that $b = [0]$ and the last one says $c = [1]$. But then $[1] = b + c = [0]$, which is a contradiction. Therefore $f(x)$ is irreducible over $\mathbb{Z}_2$.

(iv) Let $f(x) = x^3 - [9] \in \mathbb{Z}_{31}$. As in (ii), if $f(x)$ is not irreducible, then $f(x)$ must have a linear factor, i.e., $f(x)$ has a root in $\mathbb{Z}_{31}$. But one may verify that there is no element $\alpha \in \mathbb{Z}_{31}$ such that $\alpha^3 = [9]$. Therefore, $f(x)$ is irreducible over $\mathbb{Z}_{31}$.

◊ Exercise 14.2.6. Let $f(x)$ be an irreducible polynomial over a field F. Show that the quotient ring $F[x]/(f(x))$ is a field in which F is *embedded*,[9] where $(f(x))$ is the principal ideal generated by $f(x)$.

Solution. By Corollary 14.1.15, we have that $F[x]/(f(x))$ is a field. Now define the mapping $\phi : F \longrightarrow F[x]/(f(x))$ by $\phi(a) = a + I$, where $I = (f(x))$. We show that ϕ is a monomorphism.

Let $a, b \in F$. Then $\phi(a+b) = (a+b) + I = (a + I) + (b + I)$ and $\phi(ab) = ab + I = (a + I)(b + I)$. Thus ϕ is a homomorphism. Suppose $\phi(a) = \phi(b)$ for some $a, b \in F$. Then $a + I = b + I$ which implies that $a - b \in I = (f(x))$. Now since $f(x)$ is irreducible in $F[x]$ and $a, b \in F$, I has no constant polynomial other than the zero polynomial. Thus we have $a - b = 0$. So $a = b$. Therefore, ϕ is injective and hence a monomorphism as required.

[8] Note that $x^2 + [1] = (x + [1])^2$ over $\mathbb{Z}_2$.

[9] Recall that a ring R is said to be *embedded* in another ring S if R is isomorphic to a subring of S. In particular, if R and S are fields, then S is called an *extension* of R. The given result is very much important in field theory as it provides a construction of an extension field from a given field.

♦ Exercise 14.2.7. Let $f(x)$ be an irreducible polynomial over $\mathbb{Z}_p$, where p is a prime number and $\deg f(x) = n$. Show that $\mathbb{Z}_p[x]/(f(x))$ is a field containing p^n elements.

Solution. Since $f(x)$ is an irreducible polynomial, the ideal $I = (f(x))$ is a maximal ideal. Hence $\mathbb{Z}_p[x]/I$ is a field. The field $\mathbb{Z}_p[x]/I$ consists of all cosets $g(x) + I$, where $g(x) \in \mathbb{Z}_p[x]$. Now by division algorithm there exist polynomials $q(x)$ and $r(x)$ in $\mathbb{Z}_p[x]$ such that $g(x) = q(x)f(x) + r(x)$ where either $r(x) = 0$ or, $\deg r(x) < n$. Hence,

$$\mathbb{Z}_p[x]/I = \{r(x) + I \mid \text{ either } r(x) = 0 \text{ or } \deg r(x) < n\}.$$

Let

$$T = \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in \mathbb{Z}_p[x] \mid a_i \in \mathbb{Z}_p\}.$$

Since $\mathbb{Z}_p$ has p elements, the number of such polynomials of the form $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ is p^n. Let $t_1(x), t_2(x) \in T$ such that $t_1(x) + I = t_2(x) + I$. Then $f(x) \mid (t_1(x) - t_2(x))$. Now $\deg f(x) = n$ and if $t_1(x) - t_2(x) \neq 0$, then $\deg(t_1(x) - t_2(x)) < n$. Hence $f(x) \mid t_1(x) - t_2(x)$ if and only if $t_1(x) - t_2(x) = 0$, i.e., $t_1(x) = t_2(x)$. Hence $\mathbb{Z}_p[x]/I = \{t(x) + I \mid t(x) \in T\}$ contains exactly p^n elements. Therefore, $\mathbb{Z}_p[x]/I$ is a field containing p^n elements.

◊ Exercise 14.2.8. Using the Worked Out Exercise 14.2.7 above, construct a field containing 27 elements.

Solution. By virtue of the above problem, we have to produce only an irreducible polynomial of degree 3 over $\mathbb{Z}_3$. We show that

$$f(x) = x^3 + x^2 + [2] \in \mathbb{Z}_3[x]$$

is such a choice. Since $\deg f(x) = 3$, as before, $f(x)$ fails to be irreducible only if $f(x)$ has a root in $\mathbb{Z}_3$. But $f([0]) = [2]$, $f([1]) = [4] = [1]$ and $f([2]) = [14] = [2]$. Therefore, $f(x)$ is irreducible over $\mathbb{Z}_3$. Hence the field $\mathbb{Z}_3[x]/(f(x))$ contains $3^3 = 27$ elements.

◊ Exercise 14.2.9. Prove that $x^2 + 1$ is irreducible over $\mathbb{R}$. Hence prove that $\mathbb{R}[x]/(x^2 + 1)$ is a field which is isomorphic to $\mathbb{C}$, the field of complex numbers.

Solution. There is no real number satisfying the polynomial $p(x) = x^2 + 1$. Thus $p(x)$ has no linear factor and hence no nontrivial factor over $\mathbb{R}$. Therefore $p(x)$ is irreducible over $\mathbb{R}$.

Then by Worked Out Exercise 14.2.6, we have that $\mathbb{R}[x]/\langle p(x)\rangle$ is a field, say K. We show that K is isomorphic to $\mathbb{C}$, the field of complex numbers. Define $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(f(x)) = f(i)$ for all $f(x) \in \mathbb{R}[x]$. Let $f(x), g(x) \in \mathbb{R}[x]$. Let $h(x) = f(x) + g(x)$ and $t(x) = f(x)g(x)$. Now $h(x), t(x) \in \mathbb{R}[x]$ and

$$\phi(f(x) + g(x)) = \phi(h(x)) = h(i) = f(i) + g(i) = \phi(f(x)) + \phi(g(x));$$

$$\phi(f(x)g(x)) = \phi(t(x)) = t(i) = f(i)g(i) = \phi(f(x))\phi(g(x)).$$

Hence ϕ is a homomorphism. Let $a + bi \in \mathbb{C}$. Then $f(x) = a + bx \in \mathbb{R}[x]$ and $\phi(f(x)) = a + bi$. Therefore, ϕ is a homomorphism from $\mathbb{R}[x]$ onto $\mathbb{C}$. Hence by First Isomorphism theorem, $\mathbb{R}[x]/ker\,\phi \simeq \mathbb{C}$.

Since $\phi(x^2 + 1) = i^2 + 1 = -1 + 1 = 0$, it follows that $x^2 + 1 \in ker\,\phi$. Let $f(x) \in ker\,\phi$. By division algorithm, there exist $q(x)$ and $r(x)$ in $\mathbb{R}[x]$ such that $f(x) = q(x)(x^2+1) + r(x)$, where either $r(x) = 0$ or $\deg r(x) < 2$. Then $r(x) = a + bx$ for some $a, b \in \mathbb{R}$. Now $r(x) = f(x) - q(x)(x^2+1) \in ker\,\phi$. Hence $\phi(r(x)) = 0$. Then $a + bi = 0$. Hence $a = 0$, $b = 0$. This shows that $r(x) = 0$. Hence $f(x) = q(x)(x^2+1)$. Thus we find that $ker\,\phi = \langle x^2 + 1\rangle$. This completes the proof.

◊ **Exercise 14.2.10.** Find all irreducible polynomials of degree 2 in $\mathbb{Z}_2[x]$.

Solution. Any polynomial of degree 2 in $\mathbb{Z}_2[x]$ is of the form $ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}_2 = \{[0], [1]\}$. Now $a \neq [0]$. Therefore, $a = [1]$. Then $x^2, x^2 + x, x^2 + [1]$ and $x^2 + x + [1]$ are the only polynomials of degree 2 in $\mathbb{Z}_2[x]$. Now $x^2 = xx$, $x^2 + x = x(x + [1])$ and $x^2 + [1] = (x + [1])(x + [1])$, whence we conclude that all these three polynomials are reducible. Let $f(x) = x^2 + x + [1]$. Then $f([0]) = [1] \neq 0$ and $f([1]) = [3] = [1] \neq 0$. Therefore, $f(x)$ has no root in $\mathbb{Z}_2$. Thus, $x^2 + x + [1]$ is irreducible over $\mathbb{Z}_2$.

◊ **Exercise 14.2.11.** For a prime number p, how many irreducible monic polynomials of degree 2 are there in $\mathbb{Z}_p[x]$?

Solution. Let $f(x) = x^2 + ax + b \in \mathbb{Z}_p[x]$ where $a, b \in \mathbb{Z}_p$. Since $|\mathbb{Z}_p| = p$, there are p^2 such polynomials in $\mathbb{Z}_p[x]$. Now if $f(x)$ is not irreducible, then $f(x) = (x - \alpha)(x - \beta)$ for some $\alpha, \beta \in \mathbb{Z}_p$. Now, how many such distinct products of factors occur? [10] If

[10] Certainly $(x - \alpha)(x - \beta)$ and $(x - \beta)(x - \alpha)$ are the same products of the factors.

α, β are distinct, then the number is $\binom{p}{2} = \frac{p(p-1)}{2}$ and if $\alpha = \beta$, then the number is p. Thus the total number of distinct products is

$$\frac{p(p-1)}{2} + p = \frac{p(p+1)}{2}.$$

Therefore, the required number of irreducible monic polynomials over $\mathbb{Z}_p$ of degree 2 is

$$p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}.$$

Exercises

1. Show that the following polynomials are irreducible:
   - (i) $2x^5 + 15x^3 + 10x + 5$ over $\mathbb{Z}$;
   - (ii) $x^2 + x + [1]$ over $\mathbb{Z}_2$;
   - (iii) $x^6 + x^3 + 1$ over $\mathbb{Q}$;
   - (iv) $10x^3 - 7x + 14$ over $\mathbb{Q}$;
   - (v) $2x^3 - 7x + 1$ over $\mathbb{Q}$;
   - (vi) $x^4 - 5x^2 + x + 1$ over $\mathbb{Z}$;
   - (vii) $x^4 + 2x + 2$ over $\mathbb{Q}$;
   - (viii) $x^3 + [2]x - [1]$ over $\mathbb{Z}_5$;
   - (ix) $x^2 + [1]$ over $\mathbb{Z}_7$;
   - (x) $x^3 - [9]$ over $\mathbb{Z}_{11}$.
2. Let $f(x)$ be an irreducible polynomial over $\mathbb{R}$. Show that $0 < \deg f(x) \leq 2$.
3. For every prime number p and every positive integer n, show that $x^n - p$ is irreducible over $\mathbb{Q}$.
4. Find all irreducible polynomials of degree ≤ 2 in $\mathbb{Z}_p[x]$ for $p = 3$ and 5.
5. $x^4 + 1$ is irreducible over $\mathbb{Q}$ but reducible over all $\mathbb{Z}_p$ for any prime p.
6. Let $f(x) = x^3 + [6] \in \mathbb{Z}_7[x]$. Express $f(x)$ as a product of irreducible factors in $\mathbb{Z}_7[x]$.
7. Factorize $f(x) = x^3 + x^2 + x + [1]$ in $\mathbb{Z}_2[x]$.
8. For any prime number p, show that the polynomial
$$f(x) = 1 - x + x^2 - x^3 + \cdots + (-1)^{p-1}x^{p-1}$$
is irreducible over $\mathbb{Z}$.
9. Show that the polynomial $x^7 + x^5 + [1]$ is irreducible over $\mathbb{Z}_2$ and hence prove that $x^7 - 9x^5 + 11$ is irreducible over $\mathbb{Z}$.
10. Give an example of a polynomial which is irreducible over $\mathbb{Z}$ but not irreducible over $\mathbb{Z}_2$.

15

11. † Show that $x^2 + x + [4]$ is irreducible over Z_{11}. Hence show that $Z_{11}[x]/(x^2 + x + [4])$ is a field containing 121 elements.

12. † Construct a finite field containing $n = 9$ elements. Do the same for $n = 8$.

13. † Generalize Theorem 14.2.6 for an arbitrary UFD instead of Z and prove it.

14. Find whether the following statements are true or false. Justify your answer and give counter examples whenever necessary.

   a) $Z_2[x]/(x^2 + x + [1])$ is a field.

   b) $Z_3[x]/(x^2 + x + [1])$ is a field.

   c) The ideal $(x^2 + [1])$ is prime in $Z_3[x]$.

   d) [illegible] is a field.